Qualys Web Application Scanning

Training Documents

- Download the Presentation Slides and Lab Tutorial Supplement from:
  - Qualys Sharepoint site - https://bit.ly/qsc2021-was

Lab Tutorial Supplement

- All lab activity for this course is performed in a simulated lab environment
- Please refer to the WAS Lab Tutorial Supplement for the following:
  - Link to start the lab (each lab topic has a separate link)
  - Overview of the steps performed for each topic
  - Additional supporting information

Additional Reading

- WAS Getting Started Guide - https://www.qualys.com/docs/qualys-was-getting-started-guide.pdf

- WAS API User Guide - https://www.qualys.com/docs/qualys-was-api-user-guide.pdf

Agenda

- ❑ WAS Overview
- ❑ Basic Web Application Setup and Discovery
- ❑ Advanced Web Application Setup and Scanning
- ❑ API Testing
- ❑ WAS Reporting
- ❑ Tagging and Users
- ❑ Burp and Bugcrowd Integration
- ❑ Malware Detection

Web Application Scanning Overview

WAS Overview

Automated Testing (Fault Injection)

- Submit “specially crafted” characters
- Observe the server’s response
- This represents 80 – 85% of Web app vulnerabilities

Manual Testing (BURP Integration)

- Automated tools effectively detect Web application bugs (SQL execution inside user input)
- Human beings are much better at discovering program design flaws

What Do Automated Tools Miss?

Logic Errors: Point of authentication vs. point of authorization

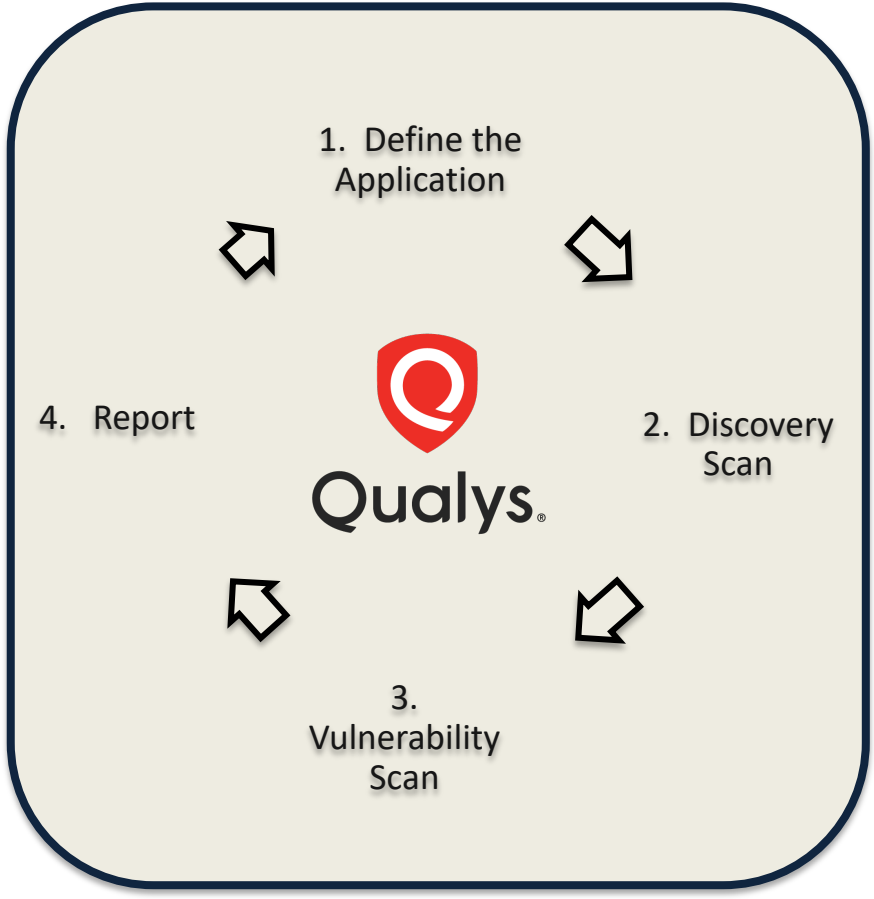
- Forced Browsing Links - user forces access to unauthorized link.

Permission Errors: File system permissions have a significant impact on application security.

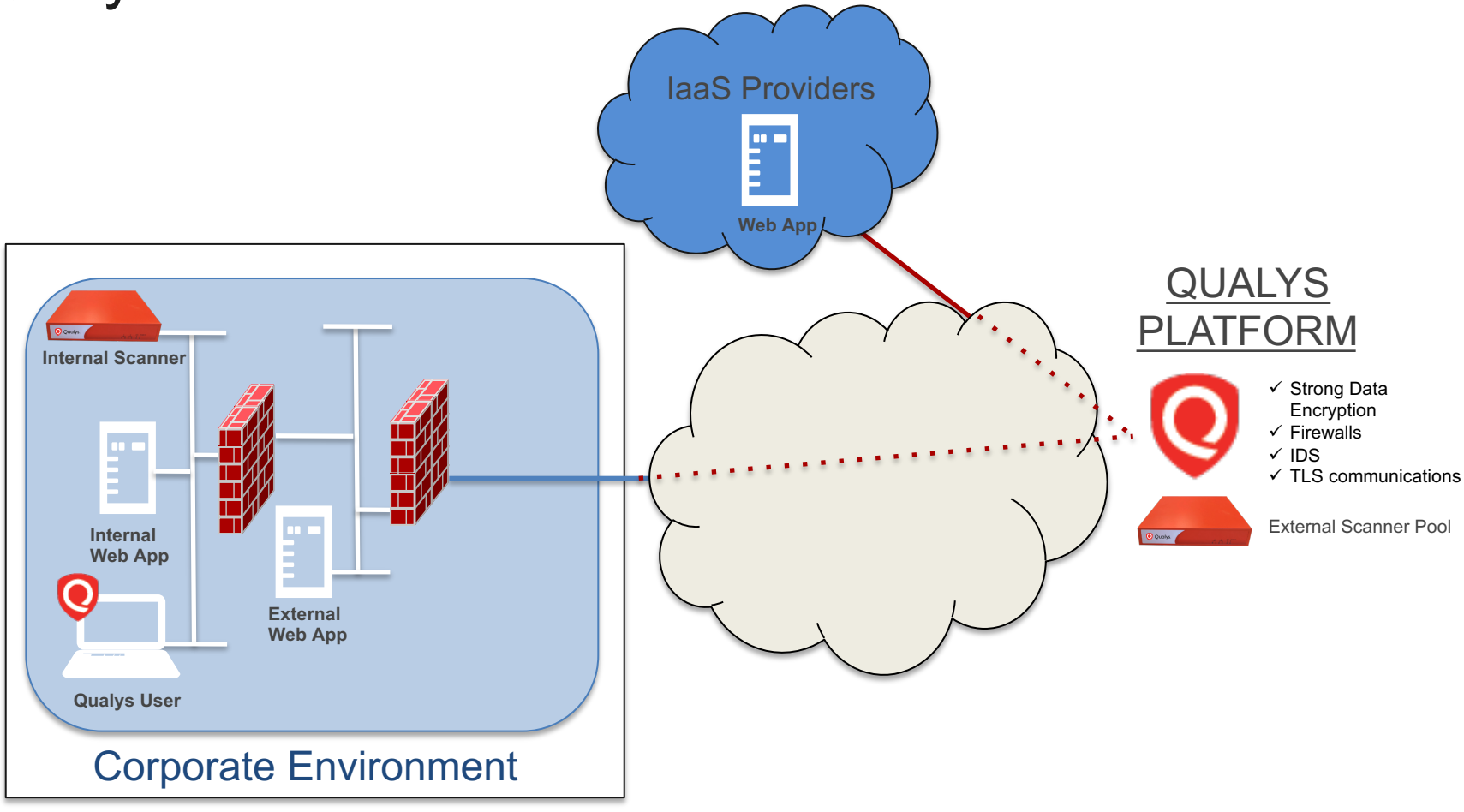
- Public file share that has employee payroll and medical records.

These typically require manual testing and detection.

Qualys WAS Lifecycle

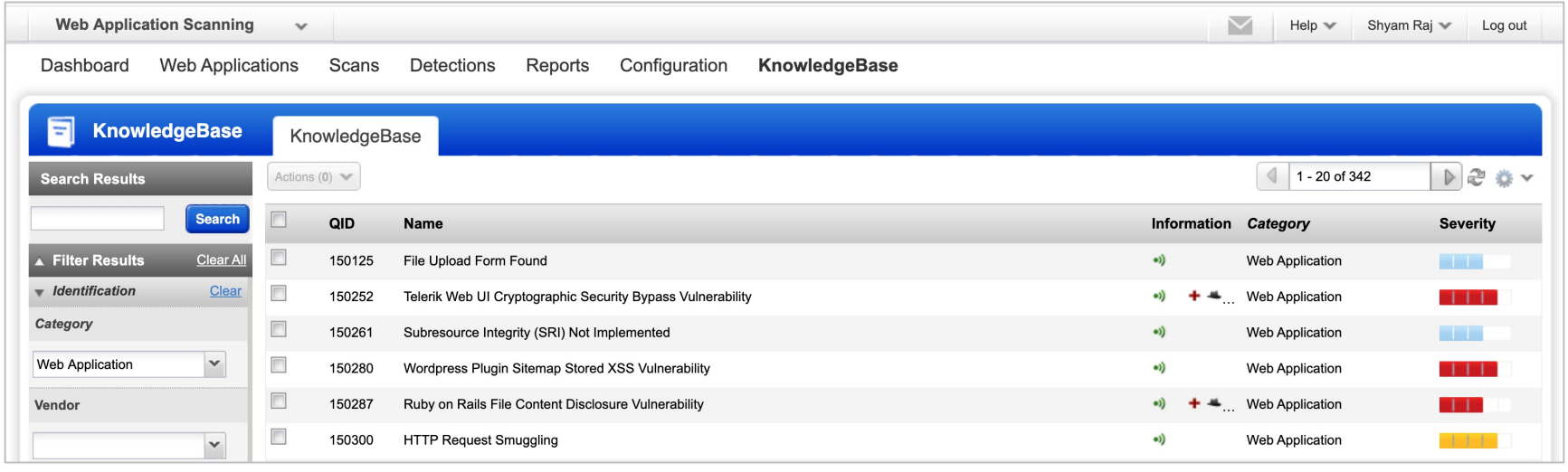


Qualys Cloud Platform



KnowledgeBase and Search Lists

What do we check for?



Web App Vulnerabilities

Confirmed Vulnerabilities

Severity	Level	Description
	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.
	Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.

Potential Vulnerabilities

Severity	Level	Description
	Minimal	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.
	Medium	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.

Sensitive Content

Severity	Level	Description
	Minimal	Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
	Medium	Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.

Information Gathered

Severity	Level	Description
	Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.
	Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.
	Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.

Search Lists Overview

User-defined Groups of QIDs

- Static search list - Manually defined
- Dynamic search list - Criteria-based

Benefits

- Dynamic List updates when new QIDs meet the search criteria
- No limitation to the number of QIDs in search list

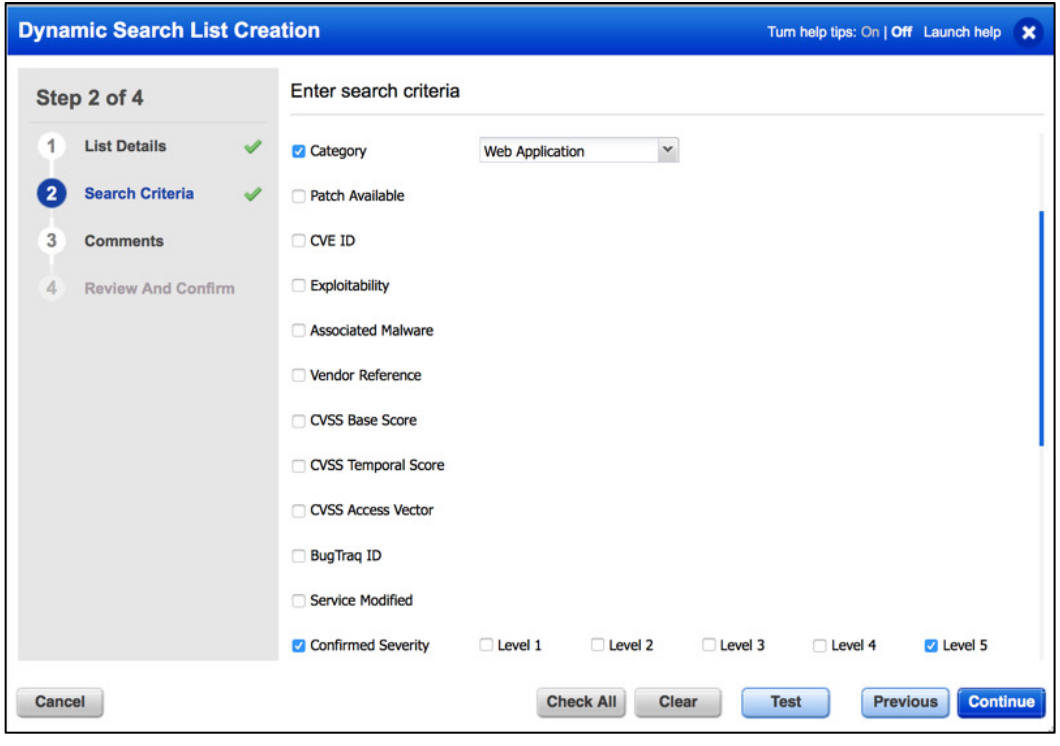
Search Lists Overview

Search lists allow you to modify the vulnerabilities for which you are:

- Scanning
- Reporting

Example:

- Run a scan for only SQLi
- Exclude a vulnerability from a scan
- Build a report for only XSS



Lab 1 and 2

Please follow **pages 3 – 5** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc2021-was

Lab 1 – KnowledgeBase

Lab 2 – Search Lists

Basic Application Setup and Discovery

Defining an Application

An application is:

- A business function typically requiring login
- Running unique code

Defining Applications – Unique Business Process

Example site:

http://site/admin/

http://site/hr/

http://site/finance/

Scenario 1:

- Each directory is part of a single app if they are part of an Intranet Portal
- (1 app total)

Scenario 2:

- Authentication credentials are different for each, with different business functions
- (3 apps total)

Defining Applications – Different ports

Example site:

E-commerce site that authenticates over https, allows browsing over http a catalog:

https://e-commerce:443/login.cgi

http://e-commerce:80/browse.cgi

Scenario:

- WAS users only need to define the *starting* port.
- The scanner will discover all ports in other links.
- (1 app total)

Defining Applications – Different Ports

Example site:

http://intranet:80/index.cgi

http://intranet:8080/index.cgi

Scenario 1:

- If the app on port 80 has links to app on port 8080
- Links are same business function (1 app total)

Scenario 2:

- If app on port 80 doesn't have links to port 8080
- Links are different business functions
- (2 apps total)

Defining Applications – Different hostnames

Example site:

http://production.domain:80/

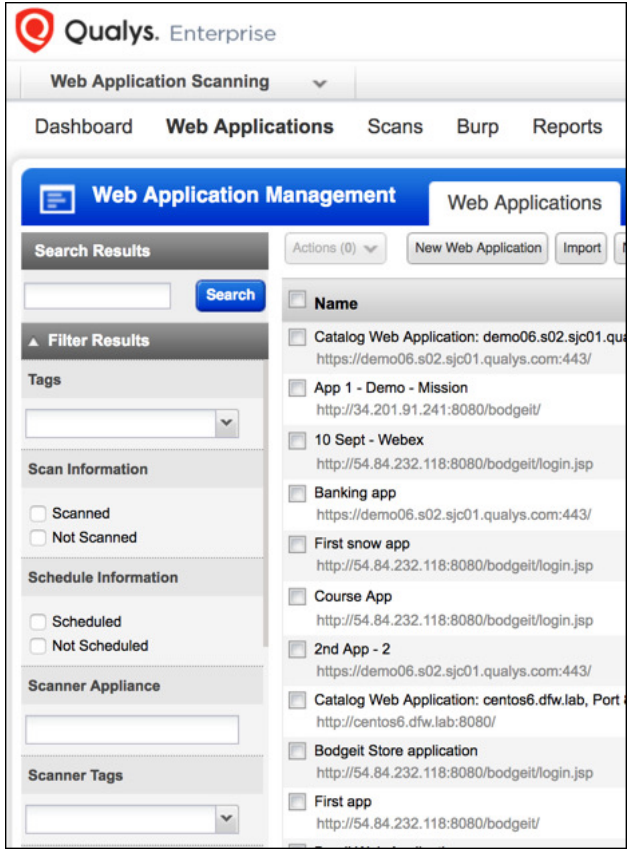
http://qa.domain:80/

Generally considered 2 applications because they are separate hostnames

Web Applications - Filtering

Filter your apps by:

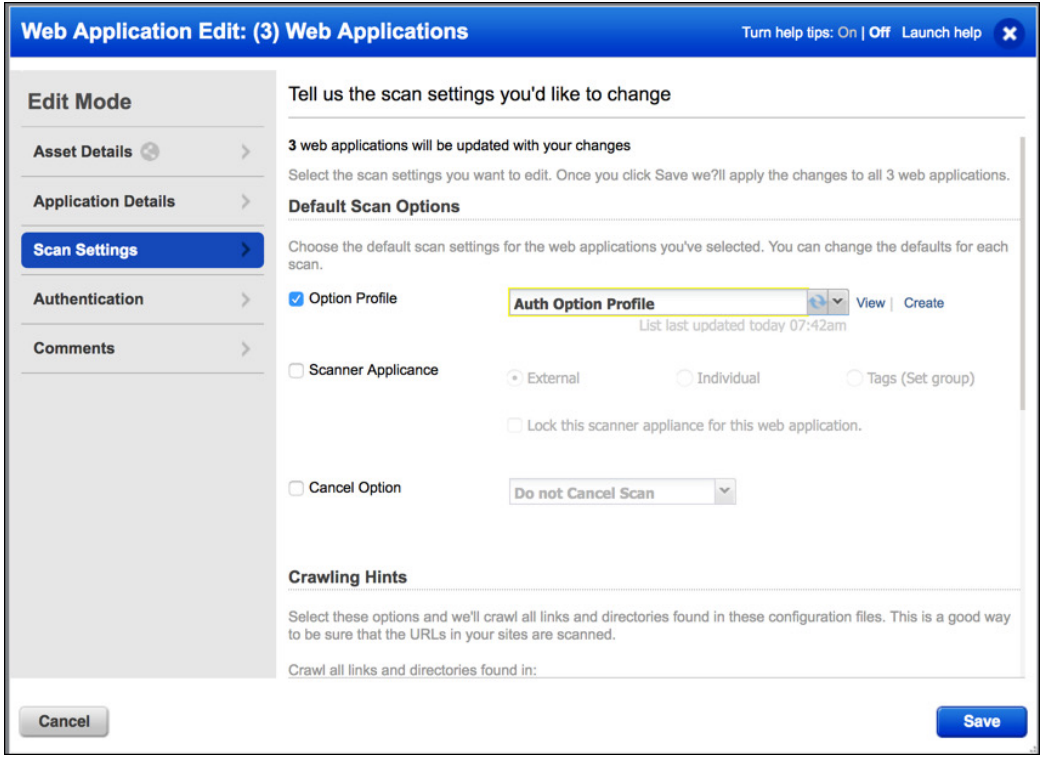
- URL
- Tags
- Scan information
- Last Scan Date
- Last Scan Status
- Scanner Appliance
- Scanner Appliance Tags
- Authentication Record
- Custom Attribute
- Creation Date



Web Applications – Bulk Edit

Bulk Edit:

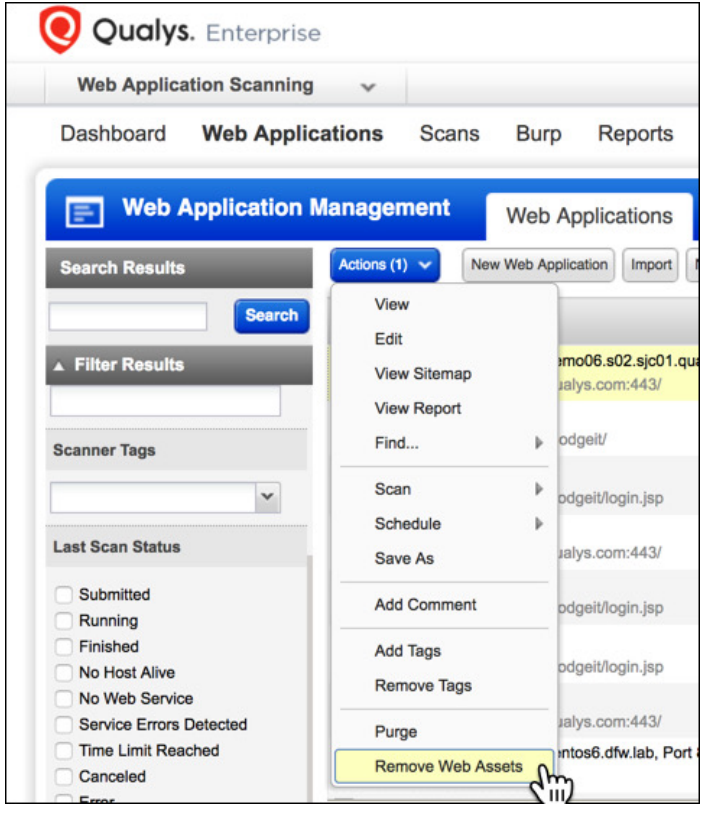
- Owner
- Scope
- Option Profile
- Scanner Appliance
- Header Injection
- Authentication Record



Removing Web Applications

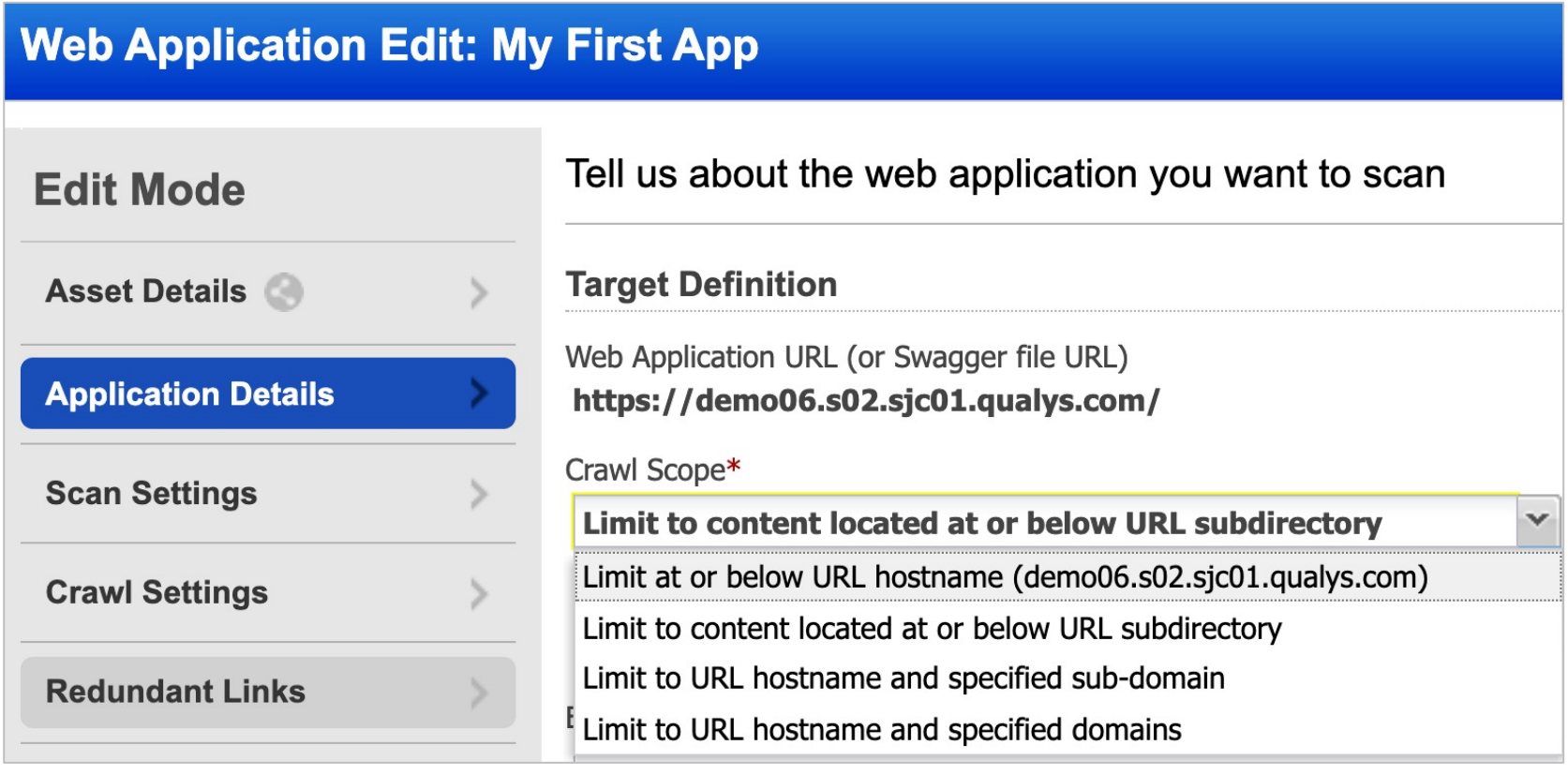
Used to remove retired Applications

Like VM, does a full purge for that web app within Qualys



Crawl Scope

Crawl Scope


Web Application Edit: My First App
Edit Mode
Asset Details
Application Details
Scan Settings
Crawl Settings
Redundant Links
Tell us about the web application you want to scan
Target Definition
Web Application URL (or Swagger file URL)
https://demo06.s02.sjc01.qualys.com/
Crawl Scope*
Limit to content located at or below URL subdirectory
Limit at or below URL hostname (demo06.s02.sjc01.qualys.com)
Limit to content located at or below URL subdirectory
Limit to URL hostname and specified sub-domain
Limit to URL hostname and specified domains

Scope – Limit to URL hostname

Select this to crawl the hostname within the URL using http or https and any port

Example: http://www.example.org/new

- All links in the http://www.example.org domain will be crawled

  http://www.example.org/support

  http://www.example.org:8080/news

- Links from www.example.org will not be followed

  http://video.www.example.org

  http://cdn.example.org

Scope – Limit to content located at or below Sub-directories

We can limit crawling to the starting URI and its sub-directories.

Sample Web Application:

Virtual Host: www.qualys.com
Port: 80
Staring URI: /research/

Using the above web application, the scanning engine will start its scan at http://www.qualys.com/research/. From this page, links will be found to:

http://www.qualys.com/research/exploits/
http://www.qualys.com/research/top10/
http://www.qualys.com/research/vulnlaws/
http://www.qualys.com/research/knowledge/
http://www.qualys.com/
http://www.qualys.com/products/qg_suite/
http://www.qualys.com/customers/
etc...

From this list of links discovered, the scanning engine will NOT crawl:

http://www.qualys.com/
http://www.qualys.com/products/qg_suite/
http://www.qualys.com/customers/

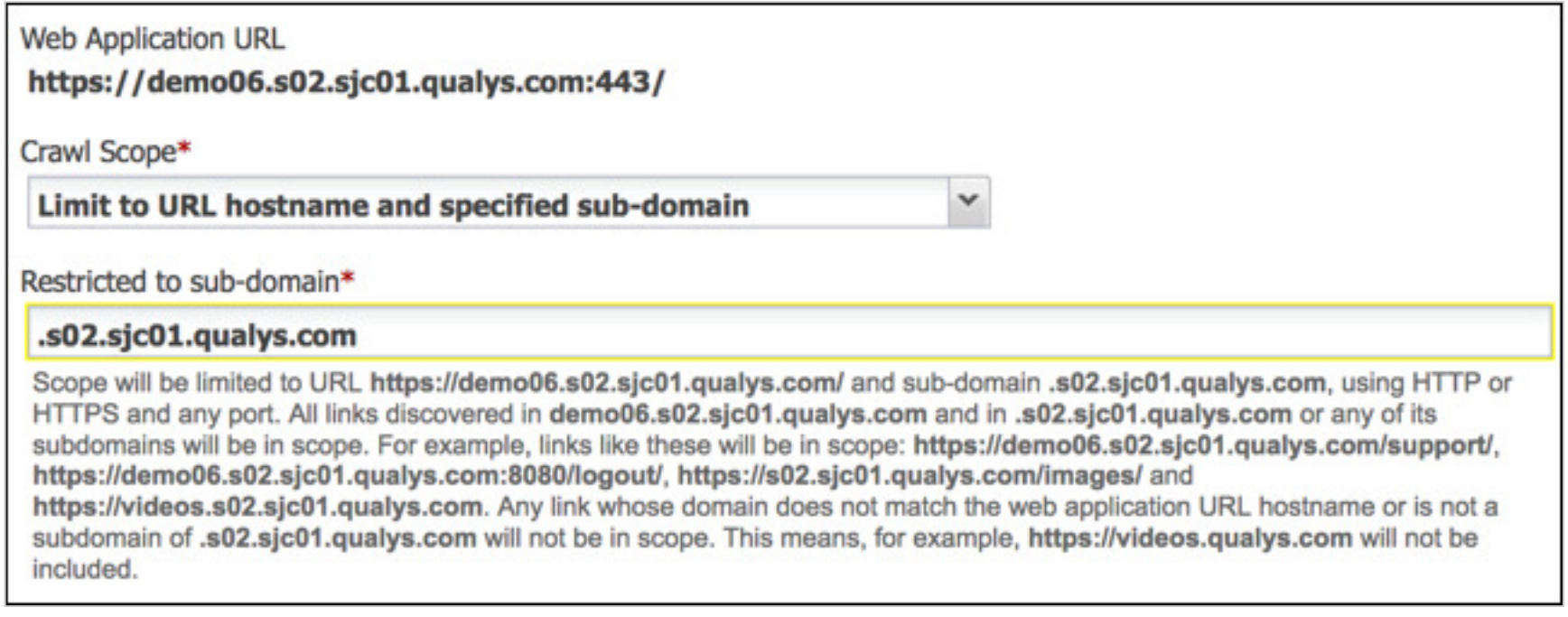
Notes:

http://www.qualys.com/ will not be crawled because it is a parent directory of /research/.

http://www.qualys.com/products/qg_suite/ and http://www.qualys.com/customers/ will not be crawled because they are not child directories of /research/.

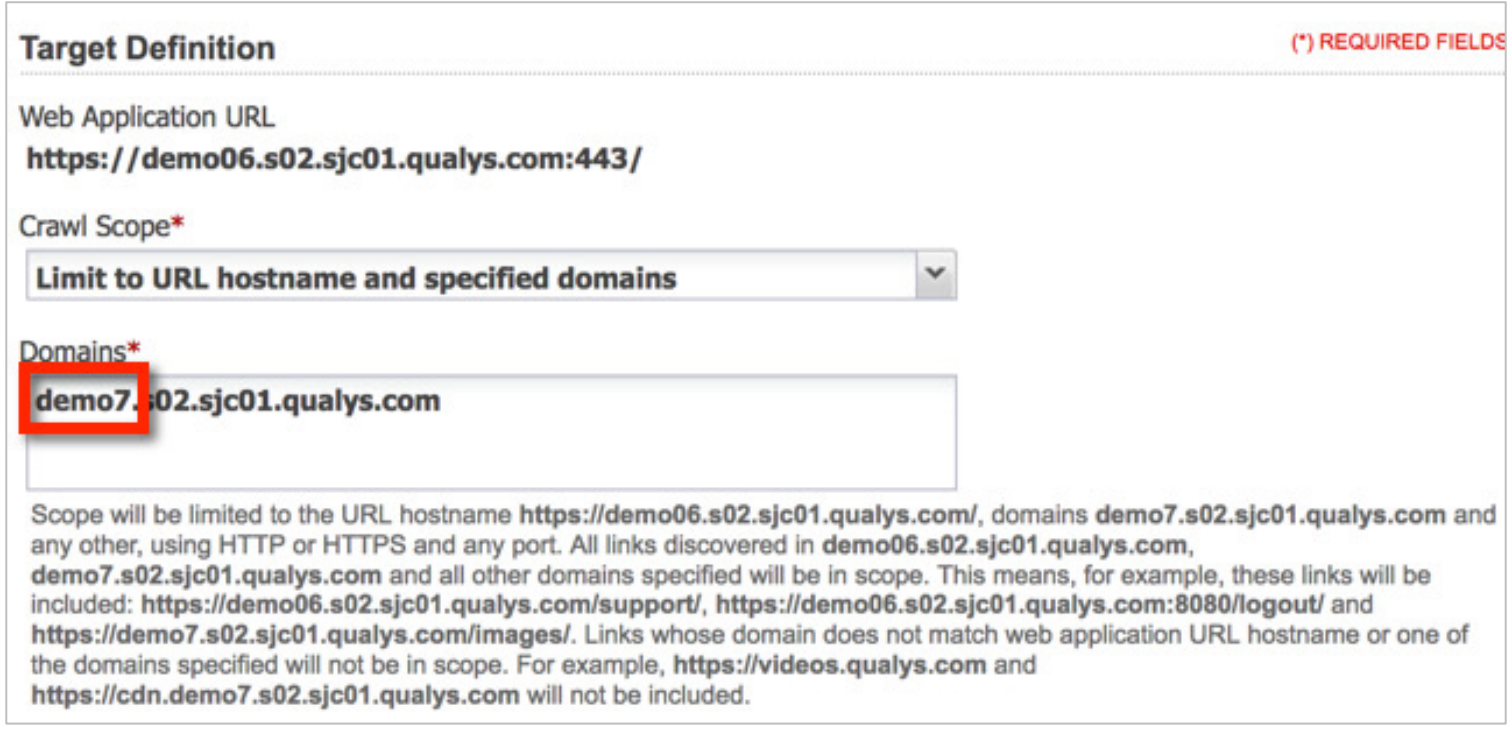
Scope – Limit to URL hostname and specified sub-domain

We can limit it to crawl only sub-domains



Scope – Limit to URL hostname and specified domains

We can crawl the starting URL, and the additional domains



Scanning

Scan Types

Discovery Scan

- All links are determined
- Authentication is maintained during the scan
- Links with forms are set aside for vulnerability assessment

Vulnerability Scan

- Should happen after at least one Discovery Scan
- Tests the web application for vulnerabilities

Discovery Scan

Discovery

1. Scan begins at starting URL identified in the application definition

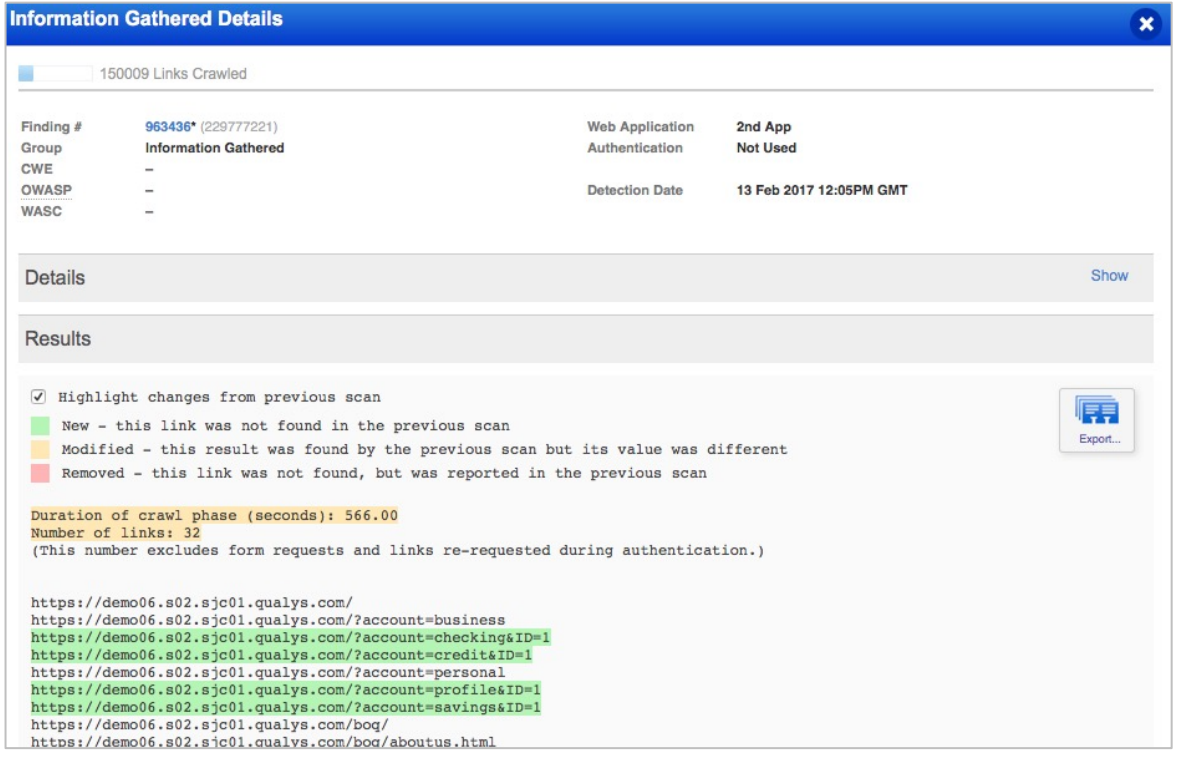
2. Using the Scope Options identified in the application definition, the scan traverses links to discover pages and content

3. Configuration data is collected from the target app and its host

4. Vulnerability testing is not performed

QID 150009 - Links Crawled

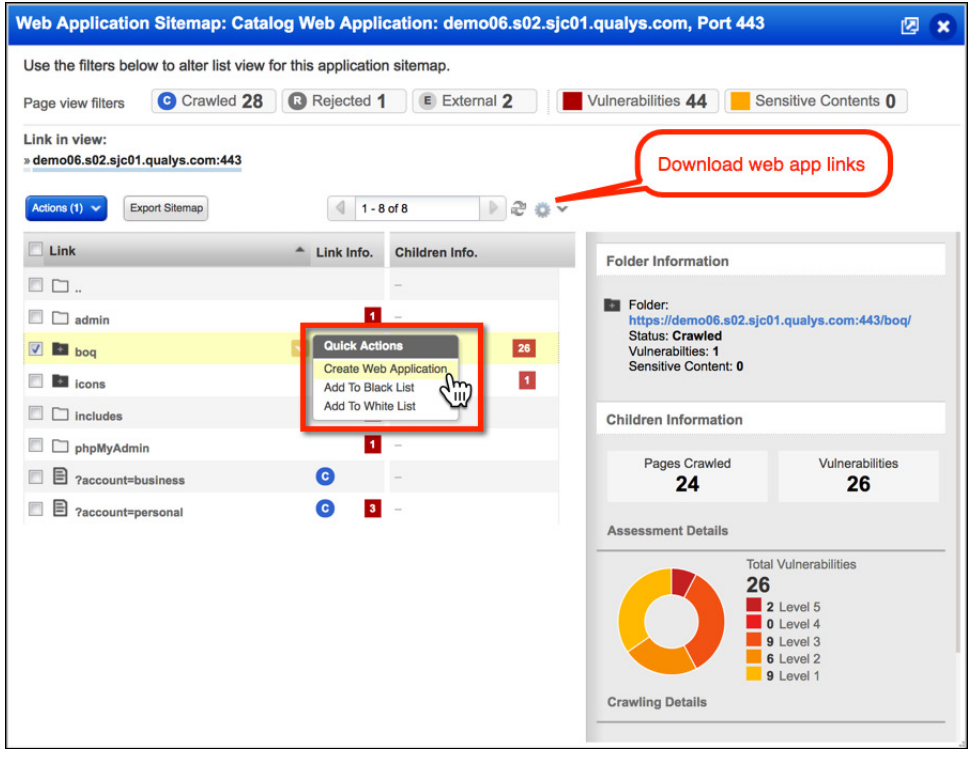
QID 150009 Links Crawled lists all links that have been crawled



Web Application Sitemap

View Web Application or Scan Sitemap To:

- View Pages Crawled and Vulnerability Statistics
- Create New Web Apps
- Add URLs to Black List
- Add URLs to White List



Lab 3, 4 and 5

Please follow **pages 5 – 14** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc2021-was

Lab 3 – Create Application 1

Lab 4 – Create Application 2

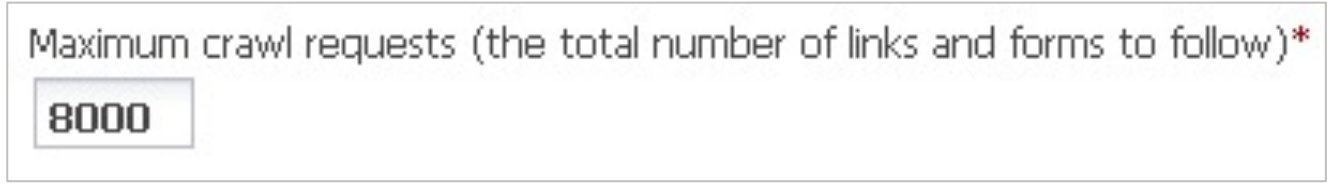
Lab 5 – Scheduled Scans

Advanced Application Setup and Scanning

Option Profile - Crawling

Crawl stops when:

- Max number of links threshold is met

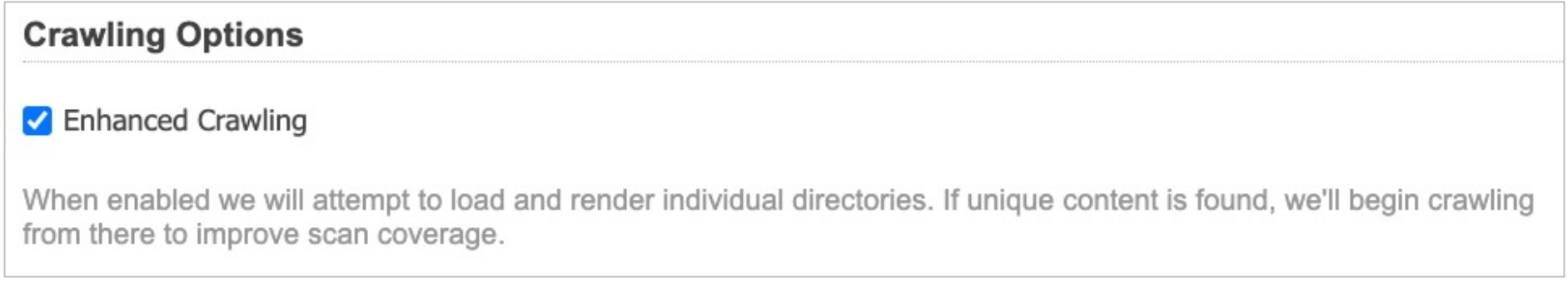


- No new links are discovered
- Scan time-out is reached

Option Profile – Scan Parameters

- Modify Form submission for GET, POST, GET&POST, None
- Change User agent
- Create Parameter sets
- Ignore common binary files
- SmartScan Support
- Change Behavior and Performance settings
- Modify Bruteforcing settings

Option Profile – Enhanced Crawling



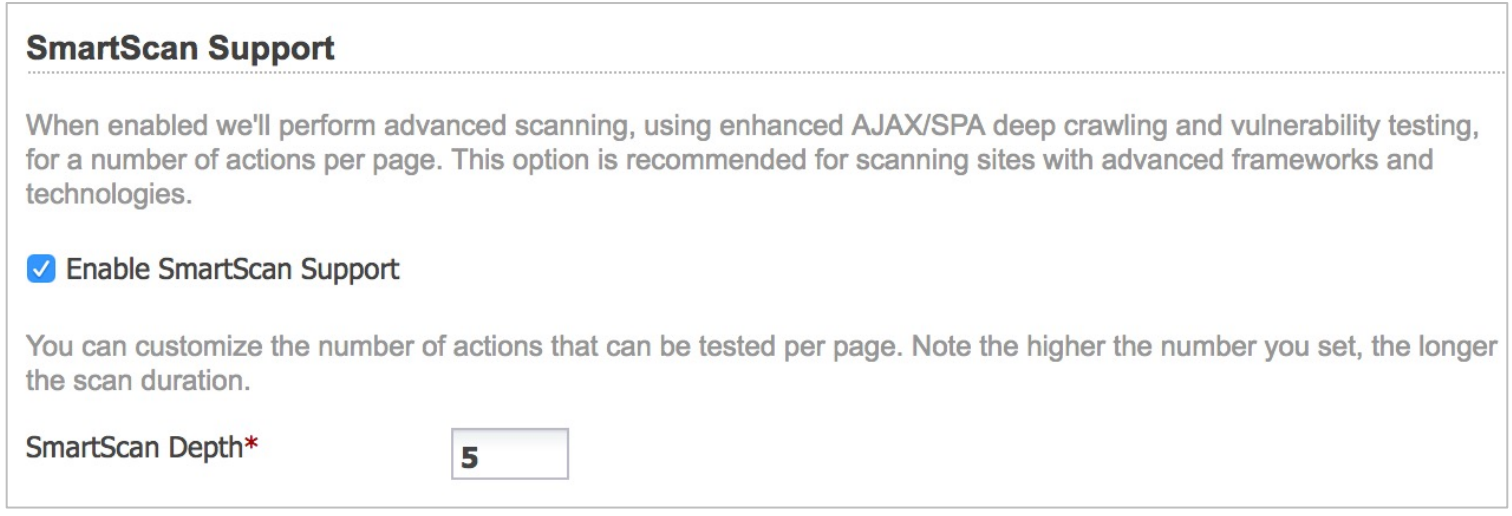
- Improves scan coverage by re-crawling individual directories present in the links found during crawling
- Uses a directory chopping approach

Option Profile – Enhanced Crawling

- Starting URL – https://www.example.com/foo/abc/xyz/register.php
- First request – https://www.example.com/foo/abc/xyz
- Then crawl – https://www.example.com/foo/abc
- Then crawl – https://www.example.com/foo

Option Profile - SmartScan

- Used for enhanced AJAX or Single Page Applications (SPA)
- Supports sites using AngularJS and bootstrap
- View QID 150148 to see links crawled – this will be your hint to verify SmartScan is working

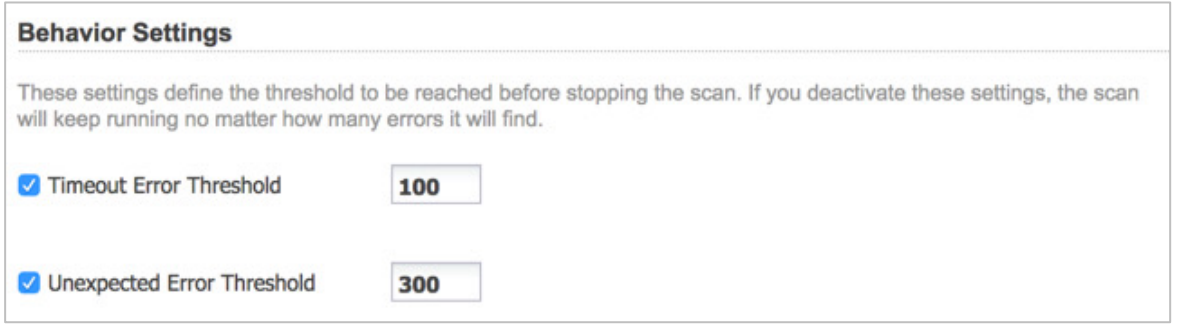


Option Profile – Behavior Settings

Timeout Error: Network connectivity or someone reboots a server

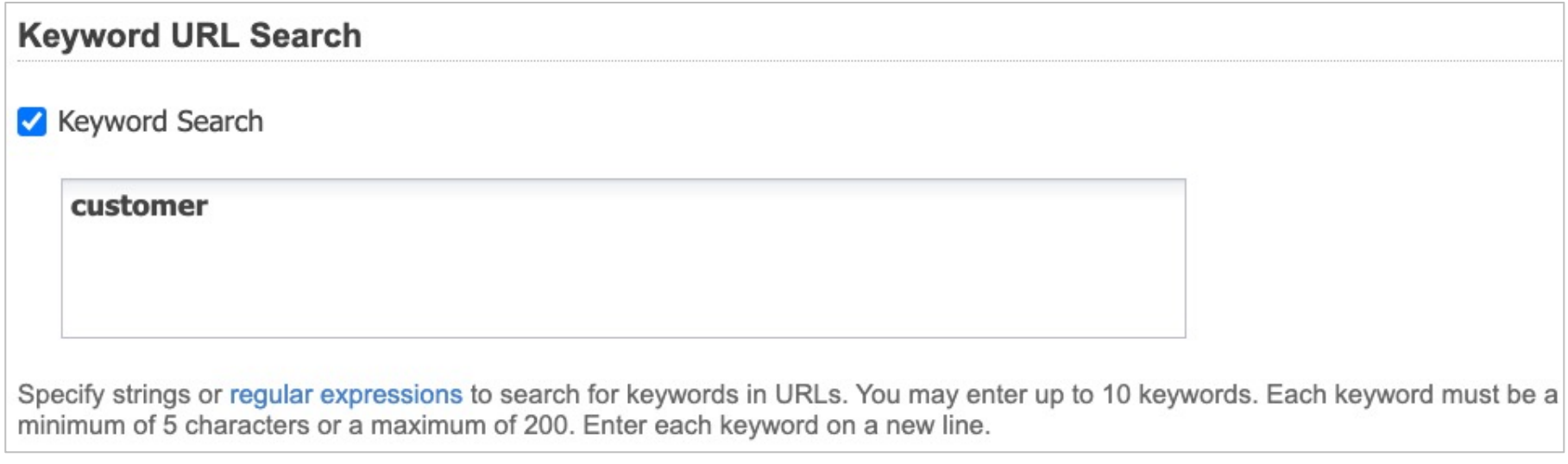
Unexpected Error: Web app returning 500/Internal Server Errors

If a threshold is met, your scan will give you a “Service Errors Detected” status



Option Profile – Keyword URL Search

- Search for URL links that contain specific keywords
- Keywords are searched in internal links during Discovery/Vulnerability scan
- Links containing the specified keyword are shown under QID 150141

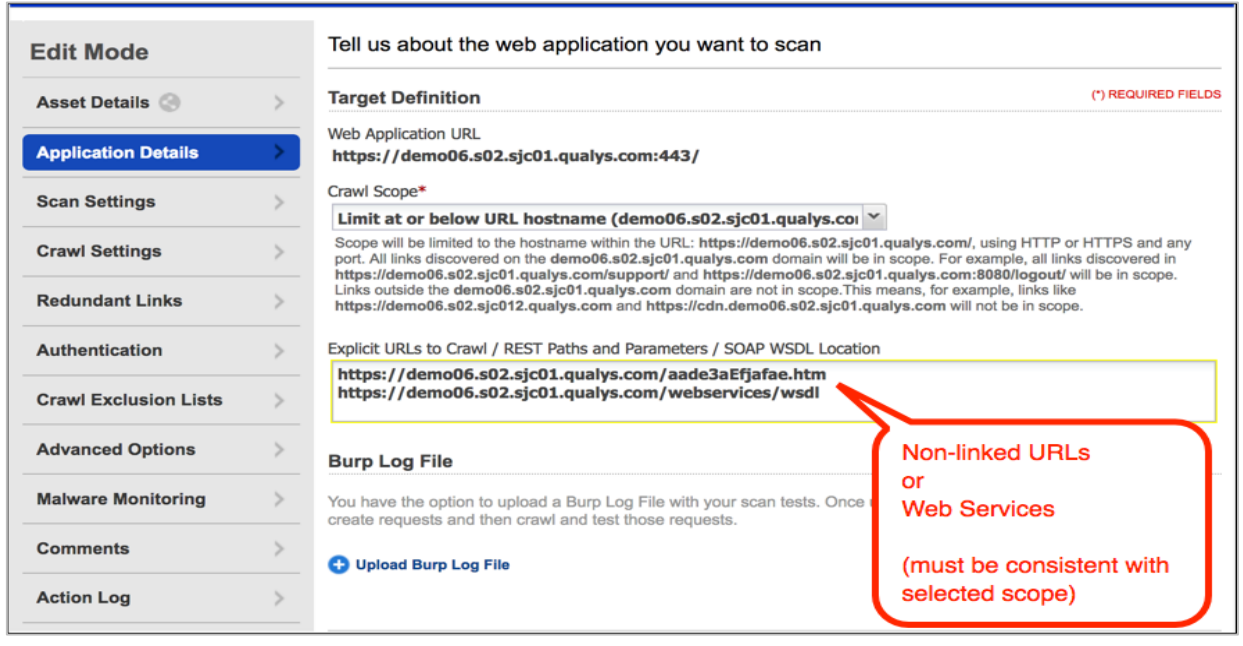


Option Profile – Bruteforcing

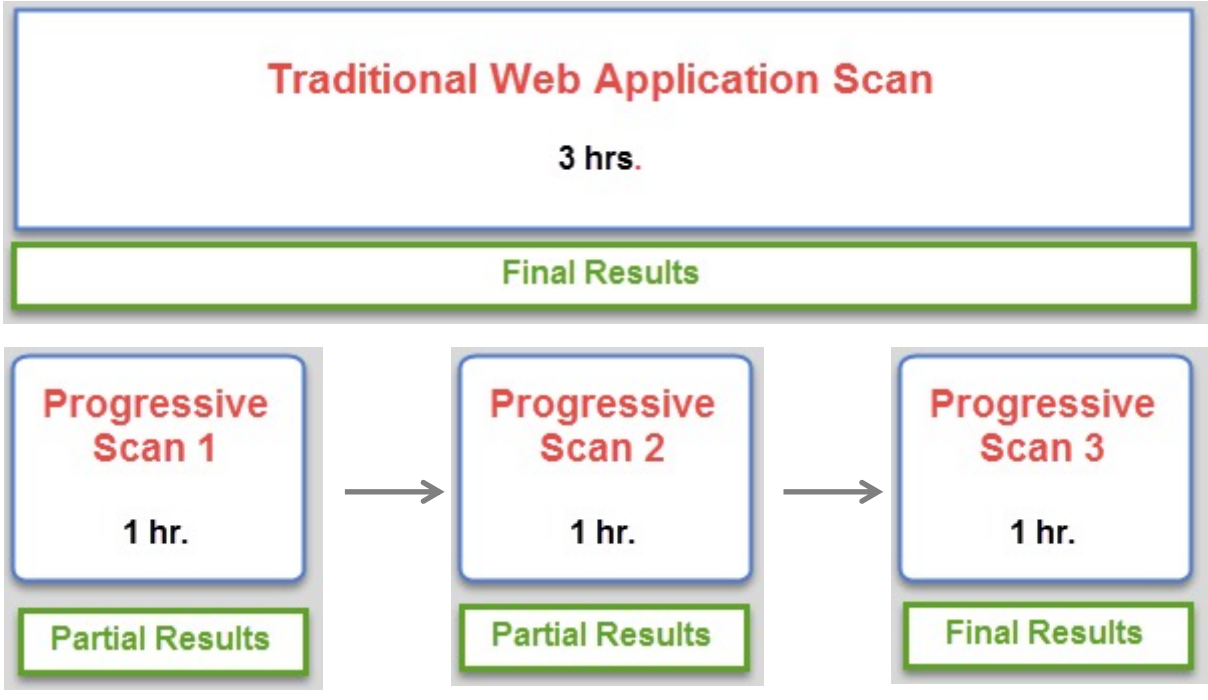
- Performed when Form Authentication is used
- Make sure you include QID 150049
- Use Qualys list or import your own

Web Application - Explicit URLs to Crawl

- Specify URLs you want the service to crawl
- Useful for pages not linked to other pages in the application



Web Application - Progressive Scanning



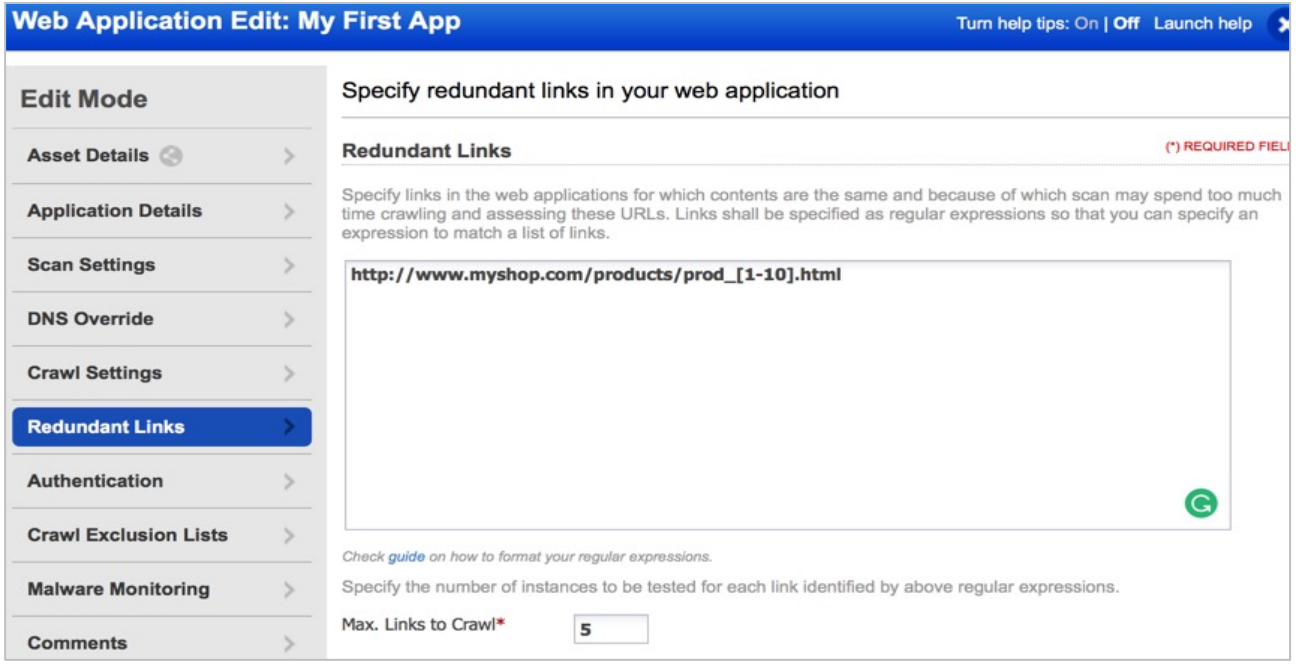
Works best with Frequently Scheduled Scans

Web Application - Progressive Scanning

- Performs ‘look back’ at previous scans
- Prioritizes pages not previously crawled
- Prioritizes new functionality
- Includes vulnerable pages detected previously
- Enhances flexibility in scheduling

Web Application - Redundant Links

Specify fully customizable patterns of redundant links so that the scan may not spend time crawling the similar links.



Web Application - Authentication

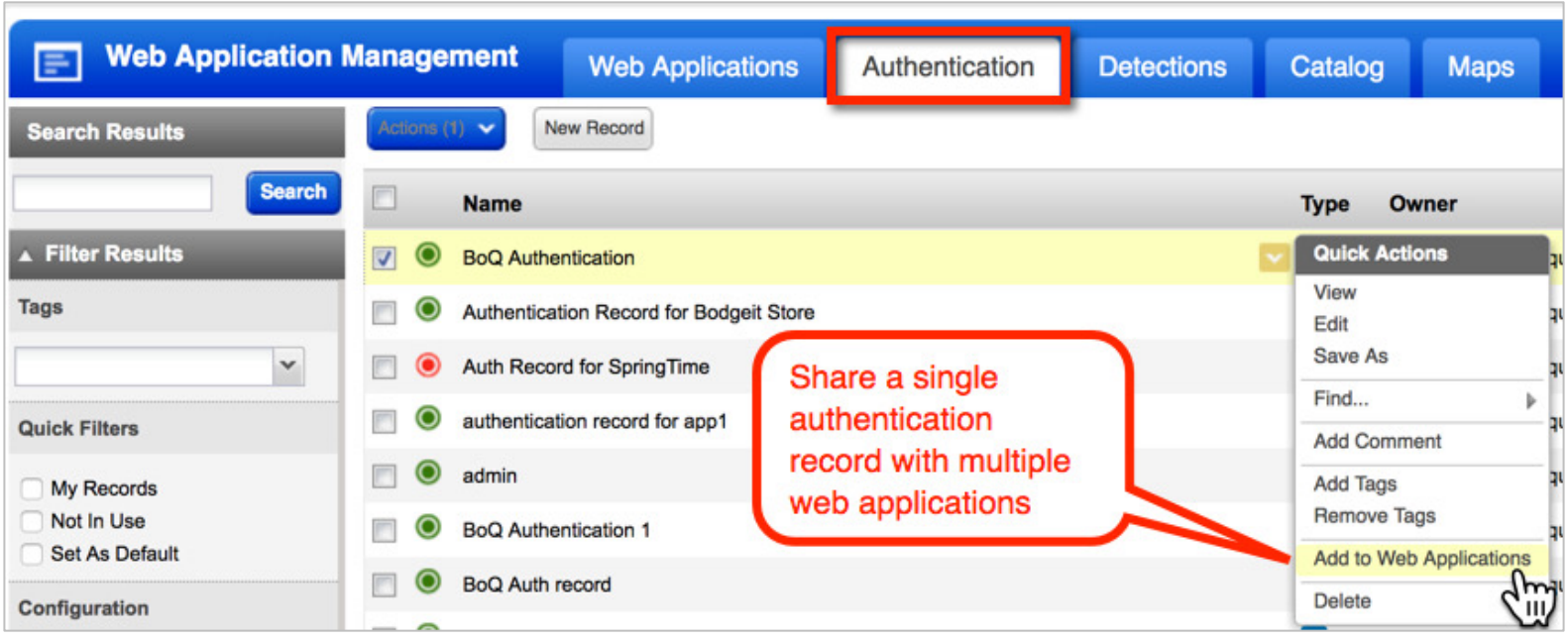
Form Records

- Standard Login
- Custom
- Selenium Script / Qualys Browser Recorder

Server Records

- Basic
- Digest
- NTLM

Manage Authentication Records



The Authentication tab provides a convenient place for managing both Form and Server authentication records.

Exclusions

White list

- Crawl specific directories or pages (within application scope).
- Content outside of ‘white-list’ is black-listed by default.
- Target a specific area of modified/updated code.

Black list

- Prevent WAS from crawling sensitive or protected locations.

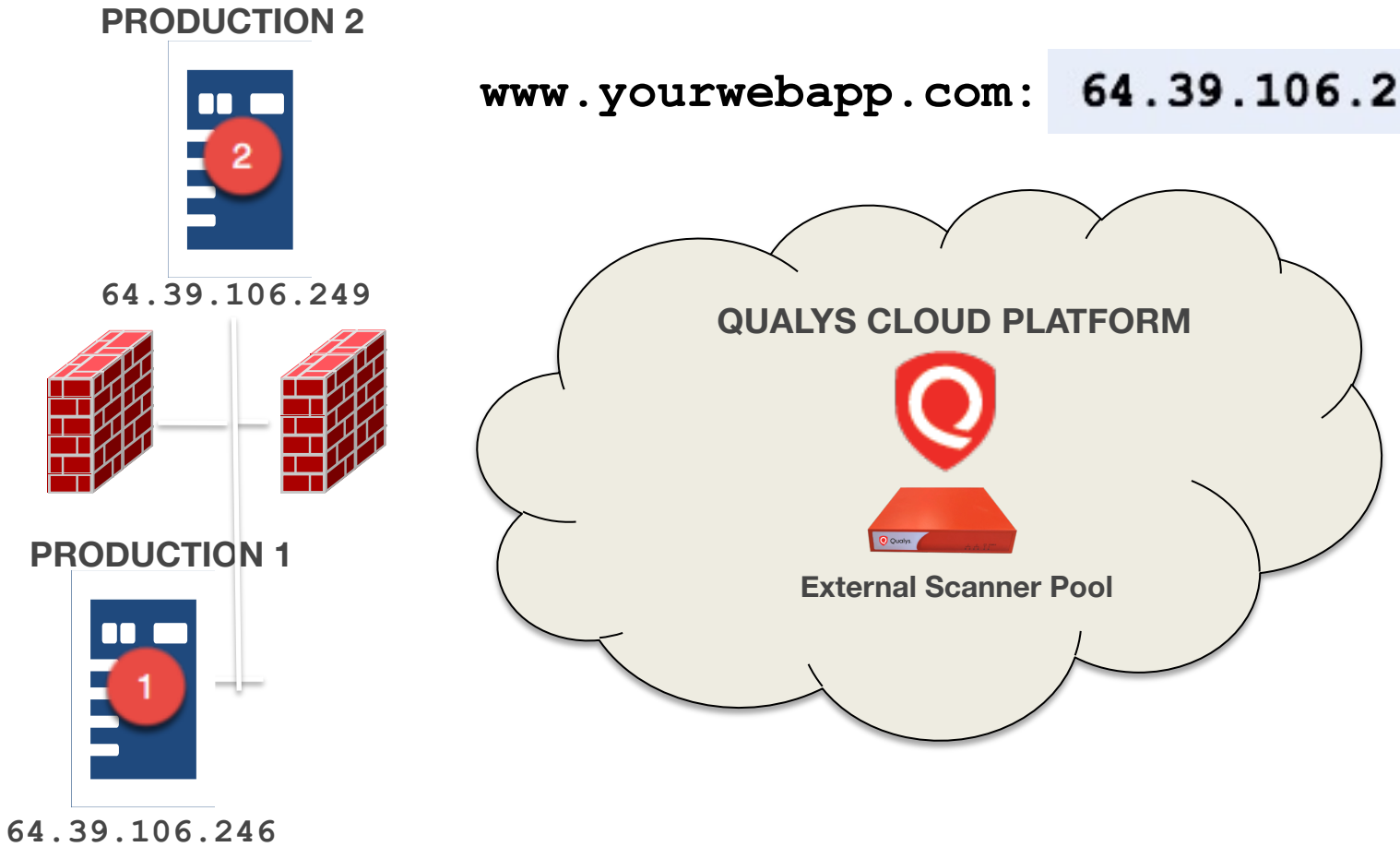
Post Data Black List

- Prevent WAS from posting HTTP forms on sensitive pages (i.e., Contact Us page).

Logout Regular Expression

- WAS scanner will not crawl to specified ’logout’ links.

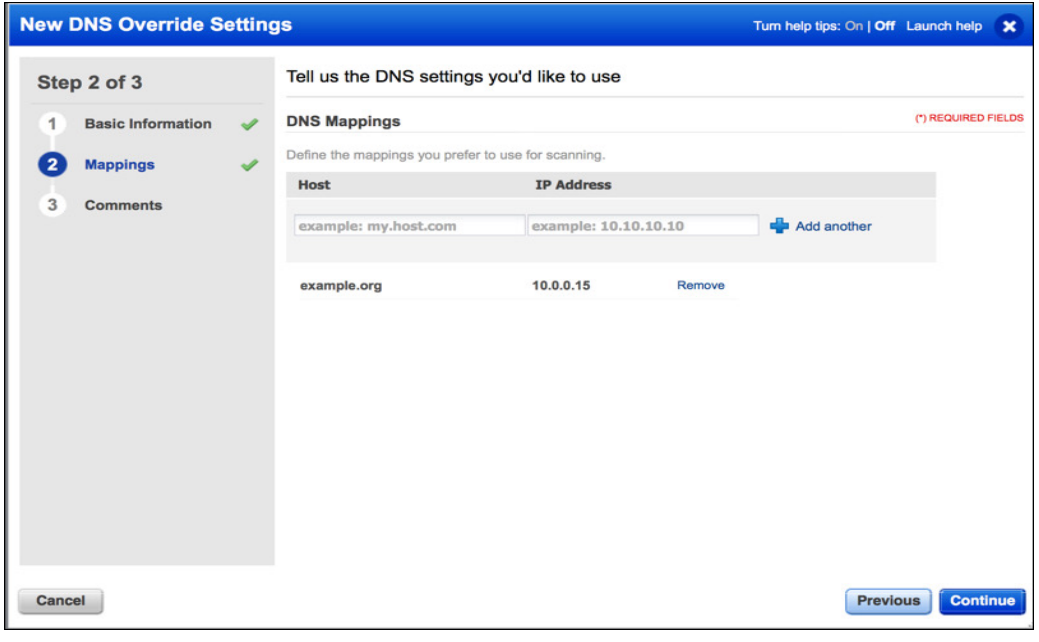
Advanced Options - DNS Override



DNS Override Settings

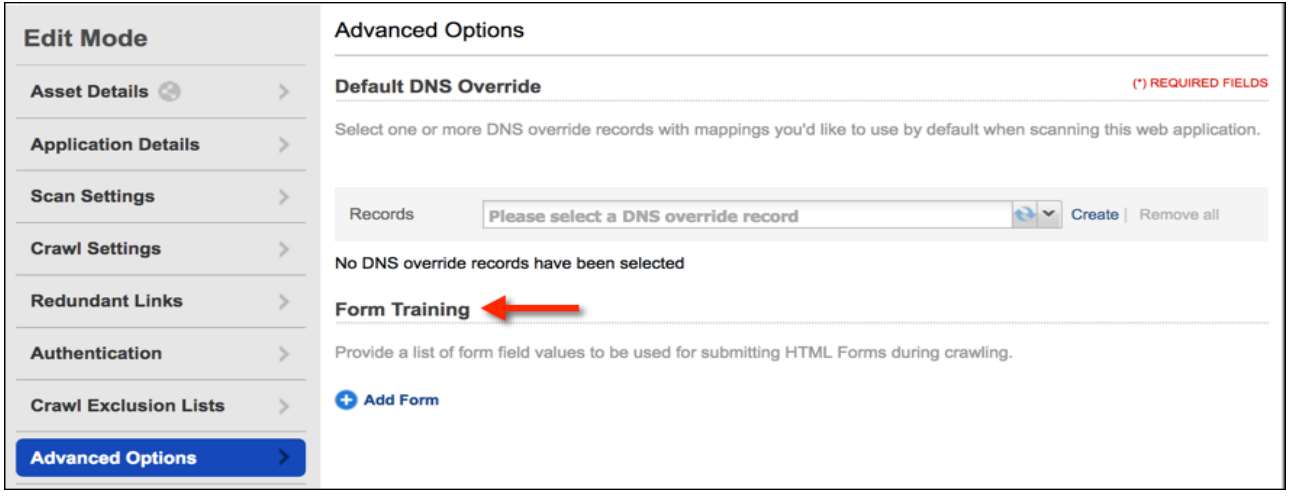
DNS Override:

- Configure if DNS not yet configured for your app that's currently in Dev or QA
- Tag to manage assignment of DNS Override



Web Application - Form Training

- This is a way for us to tell WAS what data to submit in a form, to follow a certain workflow.
- Similar to how Qualys Recorder works. Works with just about any browser.



Web Application - Path Fuzzing

Use case: For testing sites that use URL re-writing (asp.net MVC)

Example: Let us consider sports web page
http://www.abc.com/issue/17/section/sports/article/28

However, the web server will read this URL as
http://www.abc.com/search.php?issue=17&section=sports&article=28

The path fuzzing rule would be:
http://www.abc.com/issue/{issue}/section/{section}/article/{article}

No Web Service

The scan will give “No Web Service” status if the scanner:

- Cannot get a DNS lookup on the site
- Cannot reach the target because of routing
- Cannot get a web service to respond to a GET request

API Testing

APIs

- Provide a way for machine-to-machine communication

- Popular ones includes:
  - Representational State Transfer (REST) APIs
  - Simple Object Access Protocol (SOAP) APIs

- APIs use HTTP and are vulnerable to many of the same attacks as web applications

Qualys Support for SOAP APIs

- Supports basic security testing of SOAP based web services that have a Web Service Description Language (WSDL) file within the scope of the scan

- WAS uses the WSDL file to identify the web service methods and parameters supported

- WAS will attempt to perform XSS and SQL injection of the web services

Qualys Support for REST APIs

- RESTful web services can be exposed using files such as WADL (Web application description language), Swagger, or using proxy capture of the REST API client

- Qualys WAS captures the REST requests via an uploaded proxy capture of the REST API client

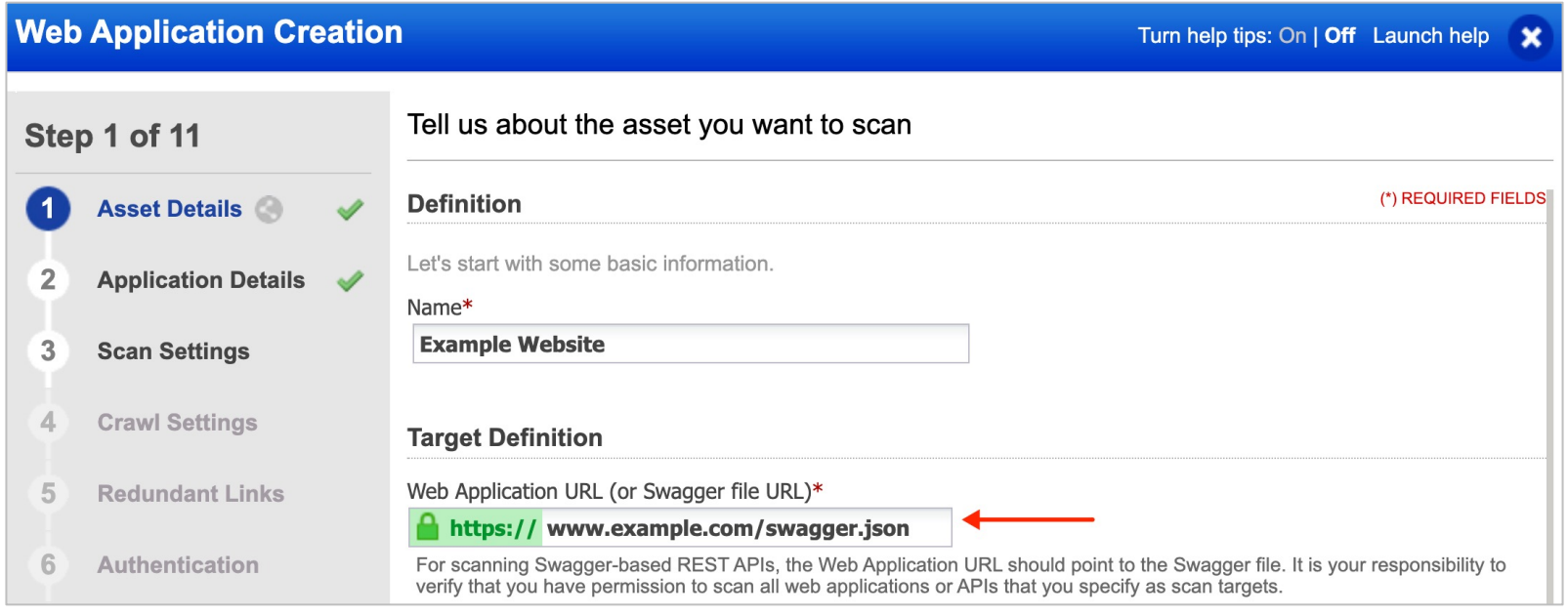
- Once the endpoints have been discovered, they can be tested for vulnerabilities

Qualys Support for openAPI (REST)

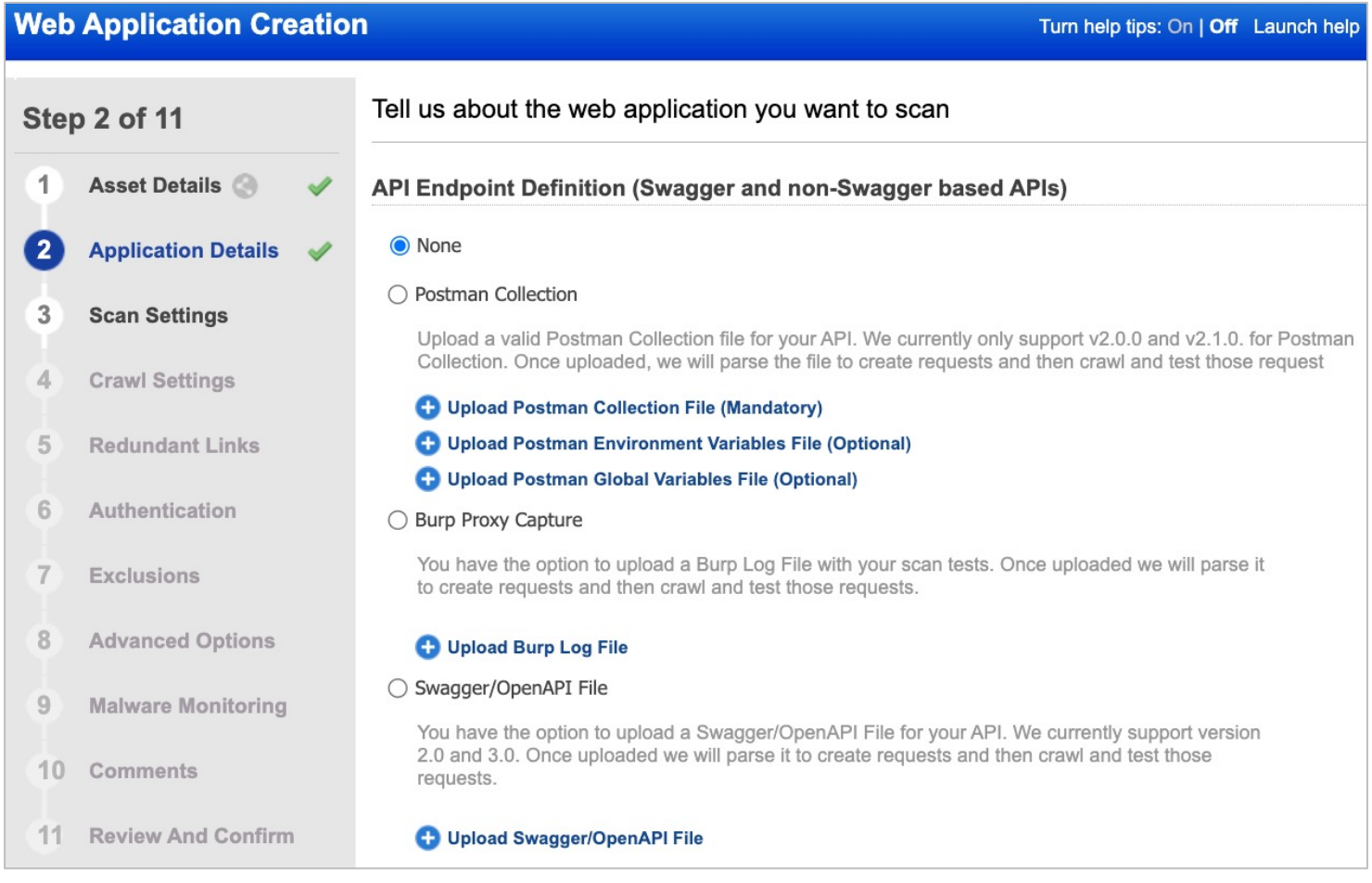
- Qualys WAS supports Swagger version 2.0 in JSON format

- If the Swagger file is available and successfully parsed, the APIs will be automatically tested for security flaws

Qualys Support for openAPI (REST)



Swagger and non-Swagger based APIs



Lab 6, 7, 8 and 9

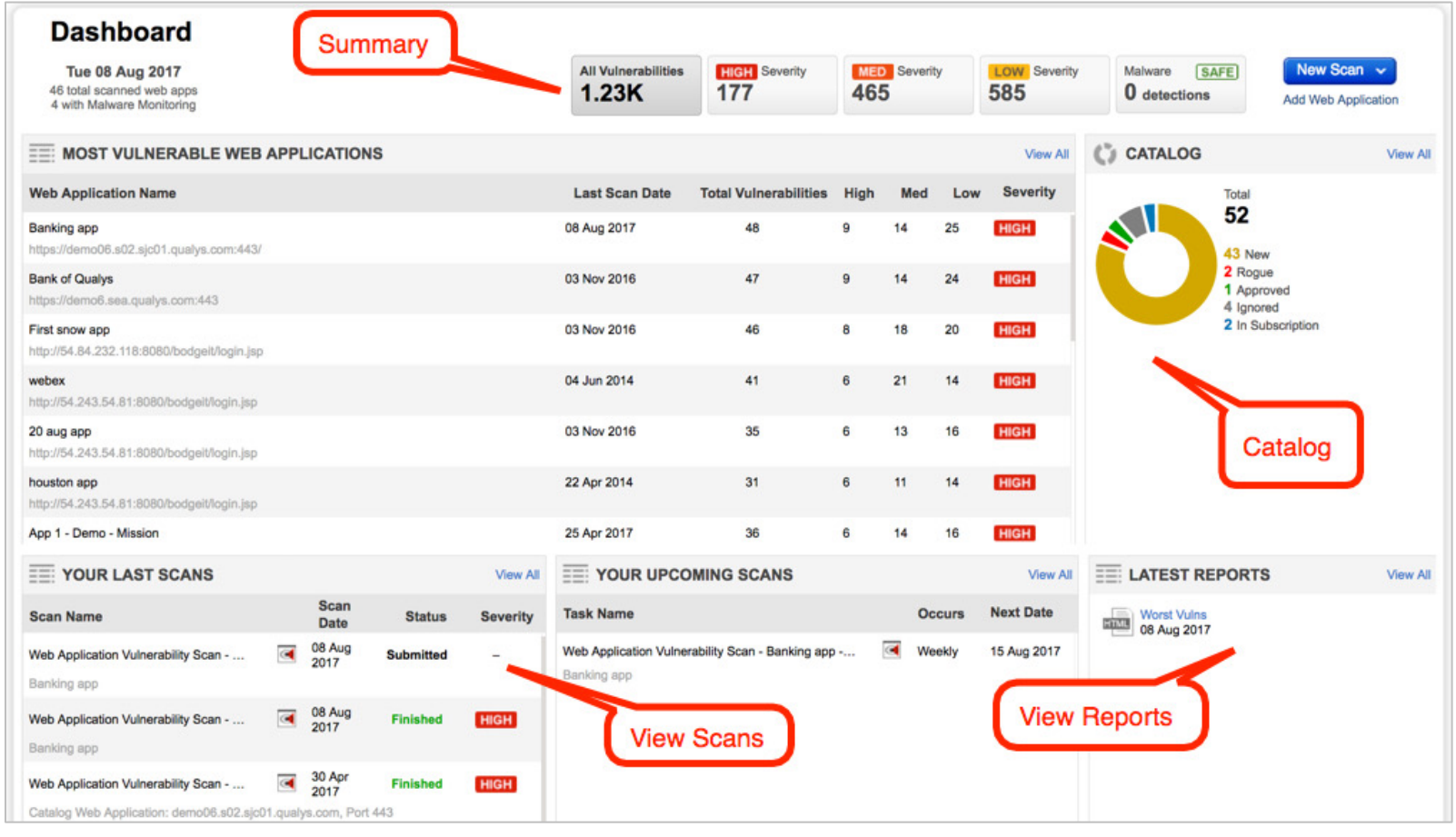
Please follow **pages 15 – 21** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc2021-was

Lab 6 – Sitemap
Lab 7 – Option Profile
Lab 8 – QBR Script 1
Lab 9 – QBR Script 2

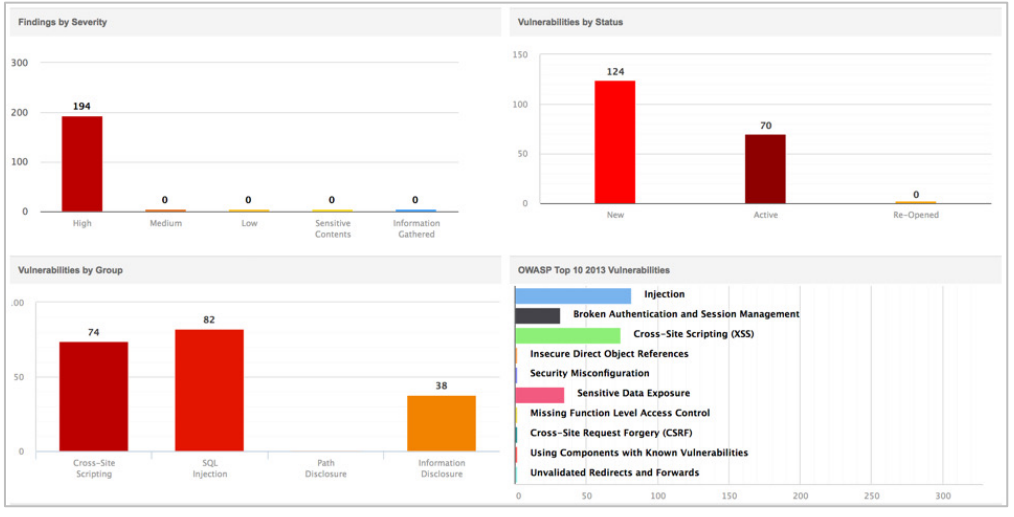
Reporting

Dashboard


Dashboard
Tue 08 Aug 2017
46 total scanned web apps
4 with Malware Monitoring
Summary
All Vulnerabilities 1.23K
HIGH Severity 177
MED Severity 465
LOW Severity 585
Malware SAFE 0 detections
New Scan
Add Web Application
MOST VULNERABLE WEB APPLICATIONS
View All
Web Application Name | Last Scan Date | Total Vulnerabilities | High | Med | Low | Severity
Banking app https://demo06.s02.sjc01.qualys.com:443/ | 08 Aug 2017 | 48 | 9 | 14 | 25 | HIGH
Bank of Qualys https://demo6.sea.qualys.com:443 | 03 Nov 2016 | 47 | 9 | 14 | 24 | HIGH
First snow app http://54.84.232.118:8080/bodgeit/login.jsp | 03 Nov 2016 | 46 | 8 | 18 | 20 | HIGH
webex http://54.243.54.81:8080/bodgeit/login.jsp | 04 Jun 2014 | 41 | 6 | 21 | 14 | HIGH
20 aug app http://54.243.54.81:8080/bodgeit/login.jsp | 03 Nov 2016 | 35 | 6 | 13 | 16 | HIGH
houston app http://54.243.54.81:8080/bodgeit/login.jsp | 22 Apr 2014 | 31 | 6 | 11 | 14 | HIGH
App 1 - Demo - Mission | 25 Apr 2017 | 36 | 6 | 14 | 16 | HIGH
CATALOG
View All
Total 52
43 New
2 Rogue
1 Approved
4 Ignored
2 In Subscription
Catalog
YOUR LAST SCANS
View All
Scan Name | Scan Date | Status | Severity
Web Application Vulnerability Scan - ... Banking app | 08 Aug 2017 | Submitted | –
Web Application Vulnerability Scan - ... Banking app | 08 Aug 2017 | Finished | HIGH
Web Application Vulnerability Scan - ... | 30 Apr 2017 | Finished | HIGH
Catalog Web Application: demo06.s02.sjc01.qualys.com, Port 443
YOUR UPCOMING SCANS
View All
Task Name | Occurs | Next Date
Web Application Vulnerability Scan - Banking app -... Banking app | Weekly | 15 Aug 2017
View Scans
LATEST REPORTS
View All
Worst Vulns 08 Aug 2017
View Reports

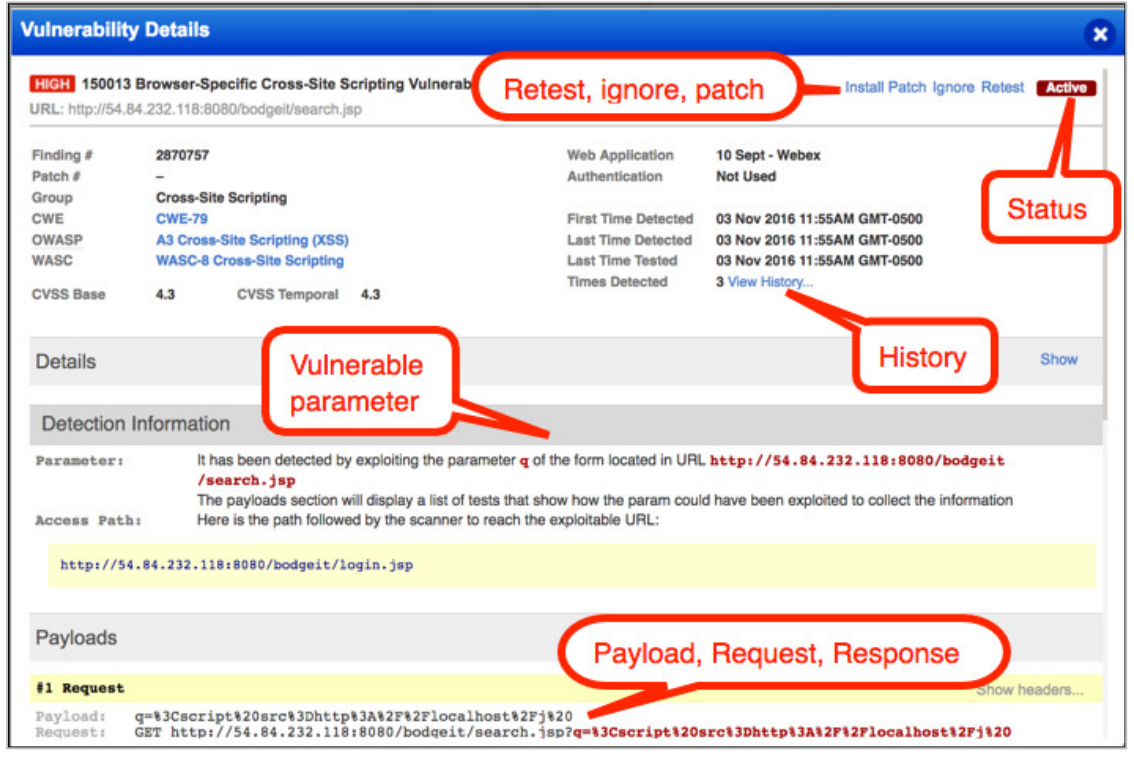
WAS Reporting

- Results listed by vulnerability, link, type, app
- Redundant results are condensed to a base cause
- Create Templates to save report formats
- Four report types
- Schedule Reports to run when you need them



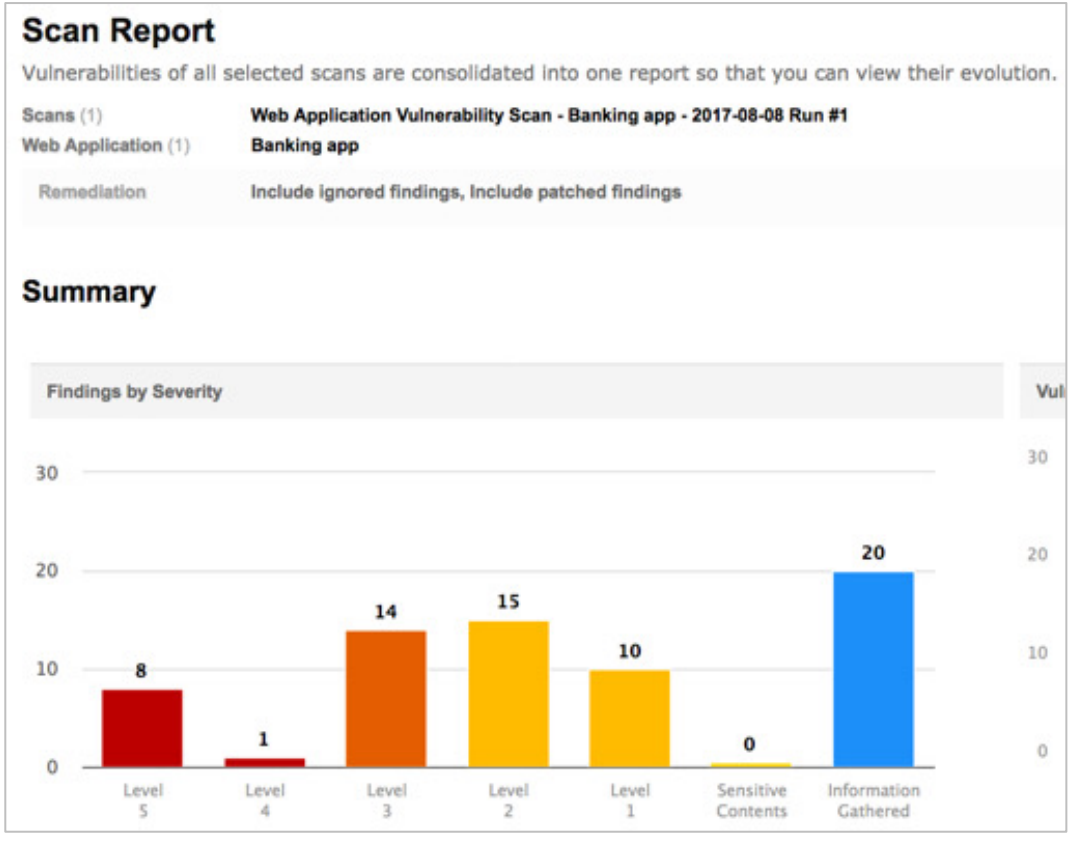
Web Application Report

- Normalized data of all scans on the web application
- Choose tags or applications for report targets
- Vulnerability Status included (New, Active, Re-opened, Fixed)
- History of vulnerability
- Retest for vulnerability



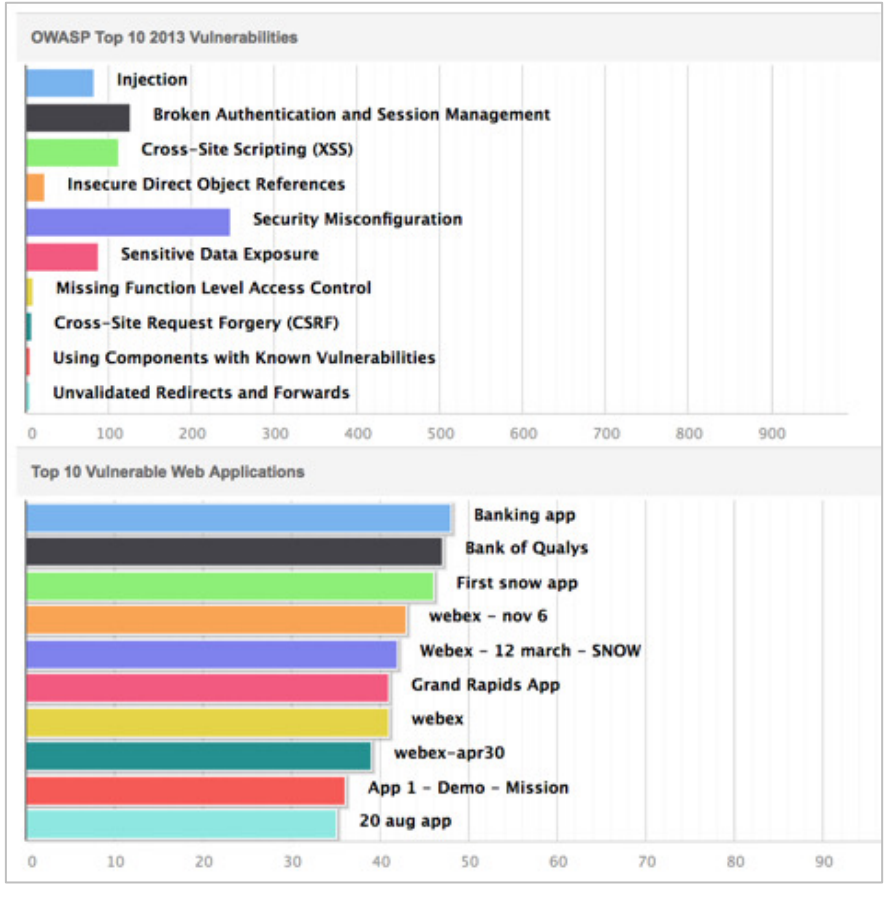
Scan Report

- Raw Scan Results
- Pick the specific scan results you'd like to view in a report
- View Threat, Impact, and Solution for vulnerabilities



Scorecard Report

- Statistics on all applications tagged in UI
- Top 10 most vulnerable applications
- OWASP breakdowns

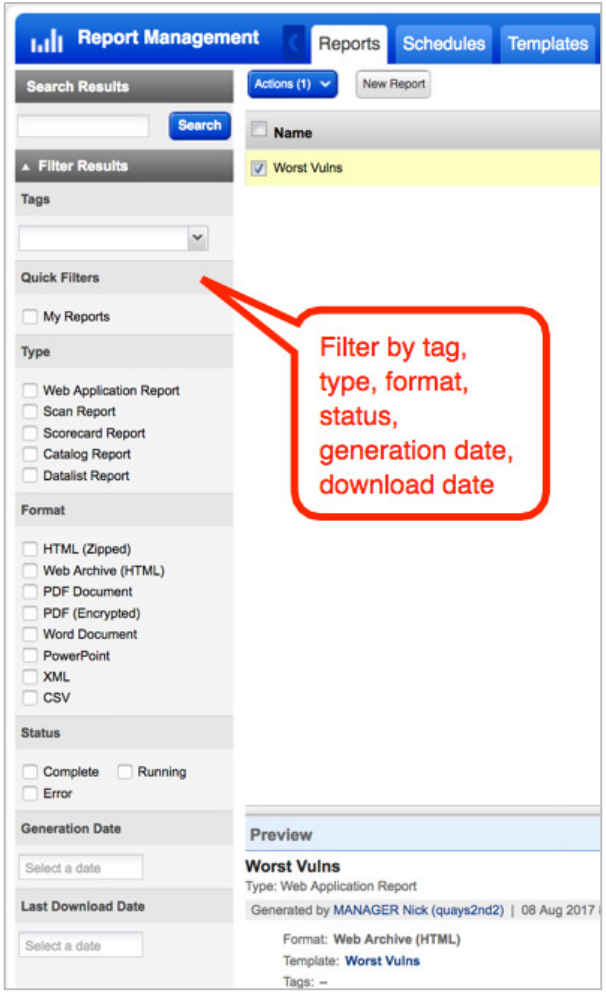


Catalog Report

- Lists web apps as New, Approved, Rogue, or Ignored
- Number of entries added over time
- Number of entries by status

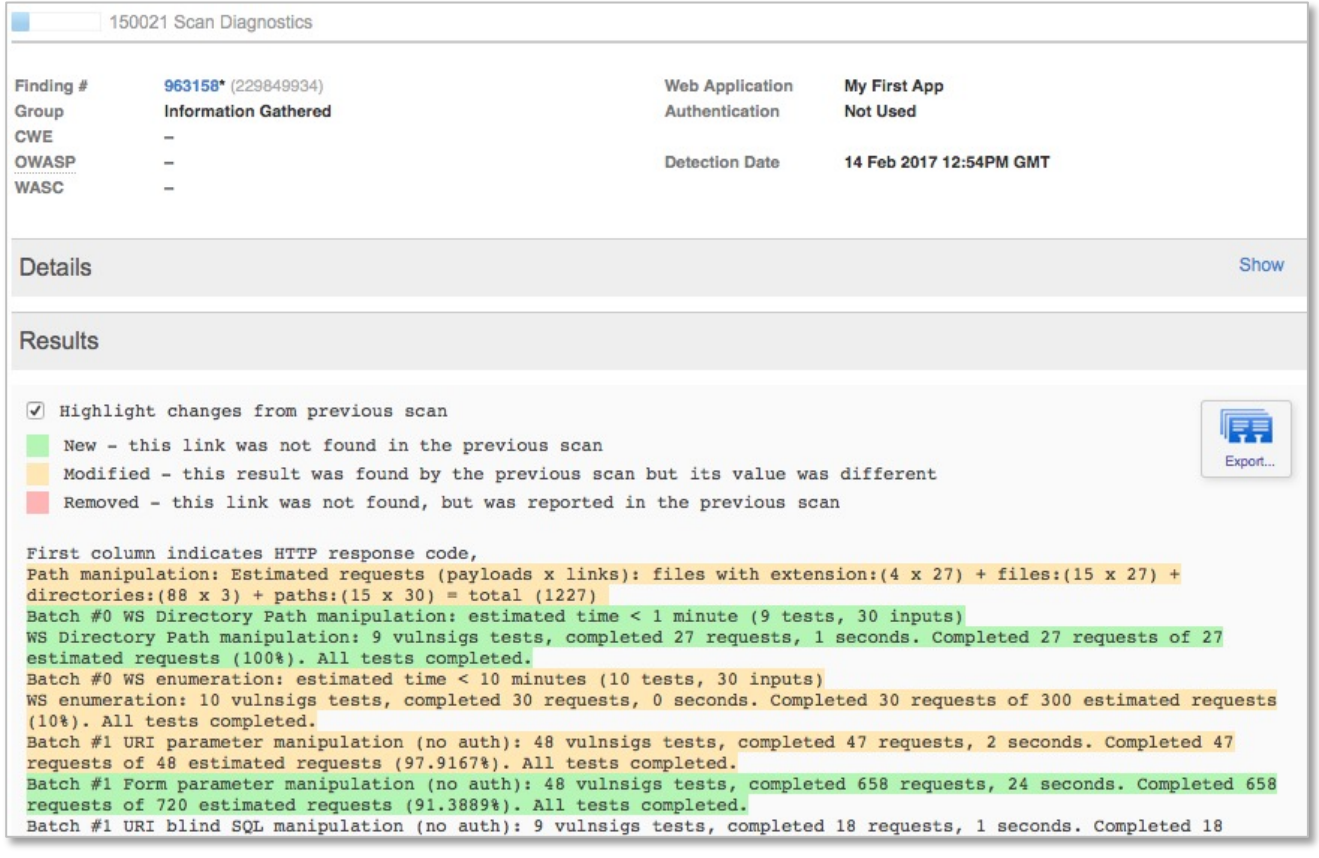
Report Management

- Create, download, run reports
- Filter existing reports
- Add tags to reports



QID 150021 – Scan Diagnostics

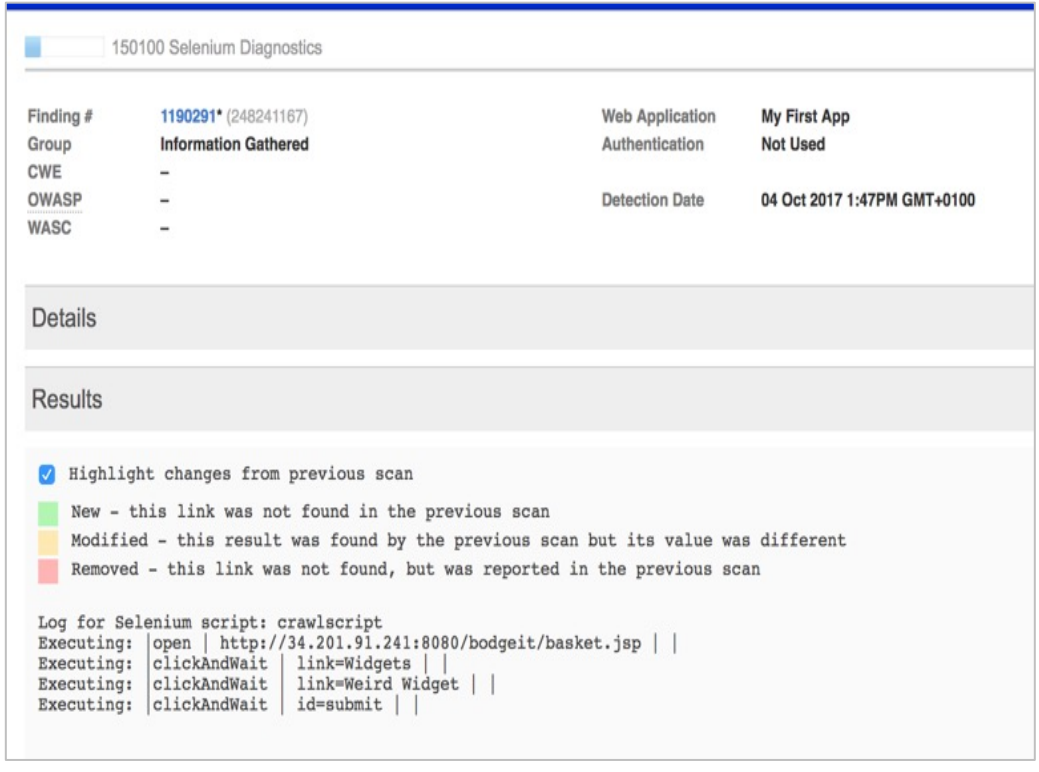
The scan diagnostics data provides technical details about the crawler's performance and behavior.



QID 150100 – Selenium Diagnostics

Troubleshoot Selenium script

See which parts of the script ran



Lab 10 and 11

Please follow **page 22** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc2021-was

Lab 10 – Web App Report
Lab 11 – Scan Report

Tags and Users

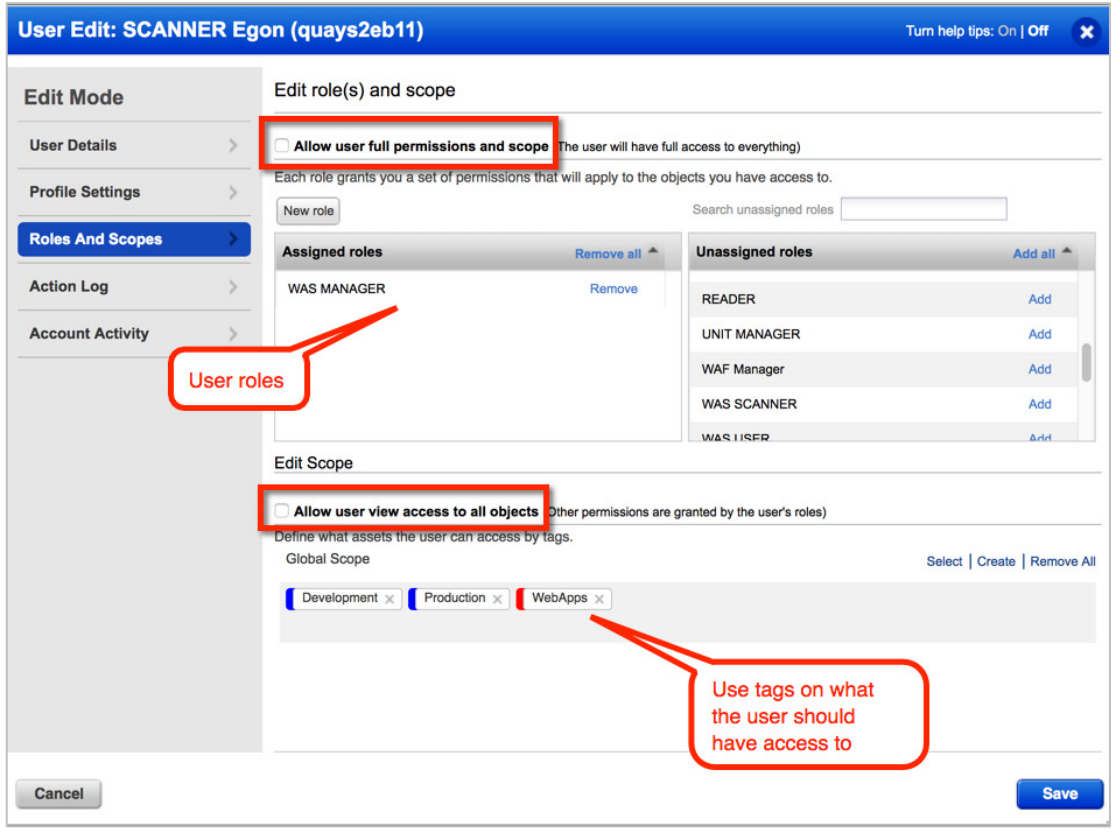
Tag Management

Add and remove tags to:

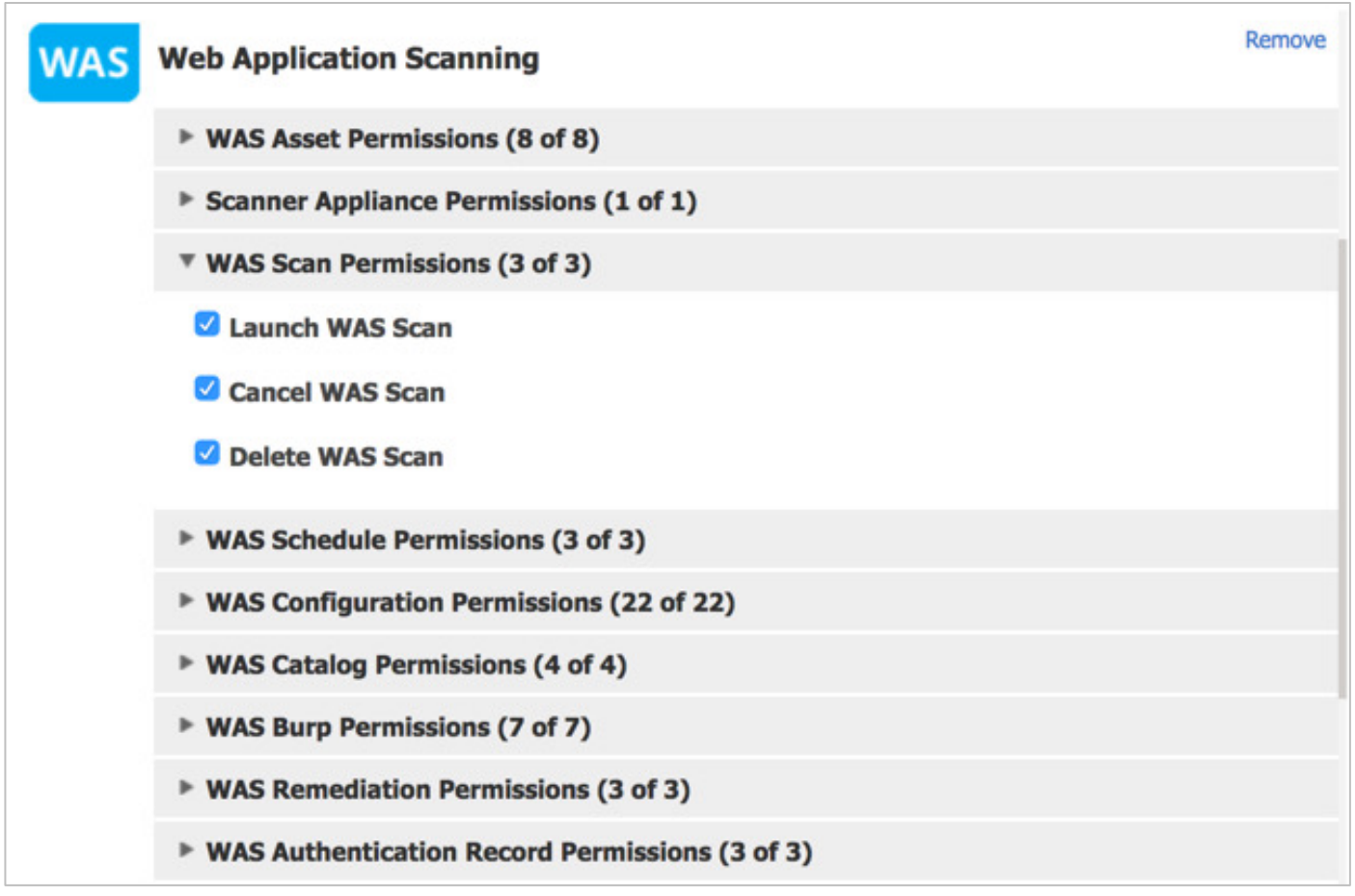
- Users
- Web Applications
- Reports
- Option Profiles
- Brute Force Lists
- Search Lists
- Scanners
- Parameter Sets
- Authentication Records

User Roles

- User roles provide privileges to access tagged assets
- Set granular permissions
- Grant QA or Developers access



Customize a role



Lab 12 and 13

Please follow **pages 23 – 26** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc21-was

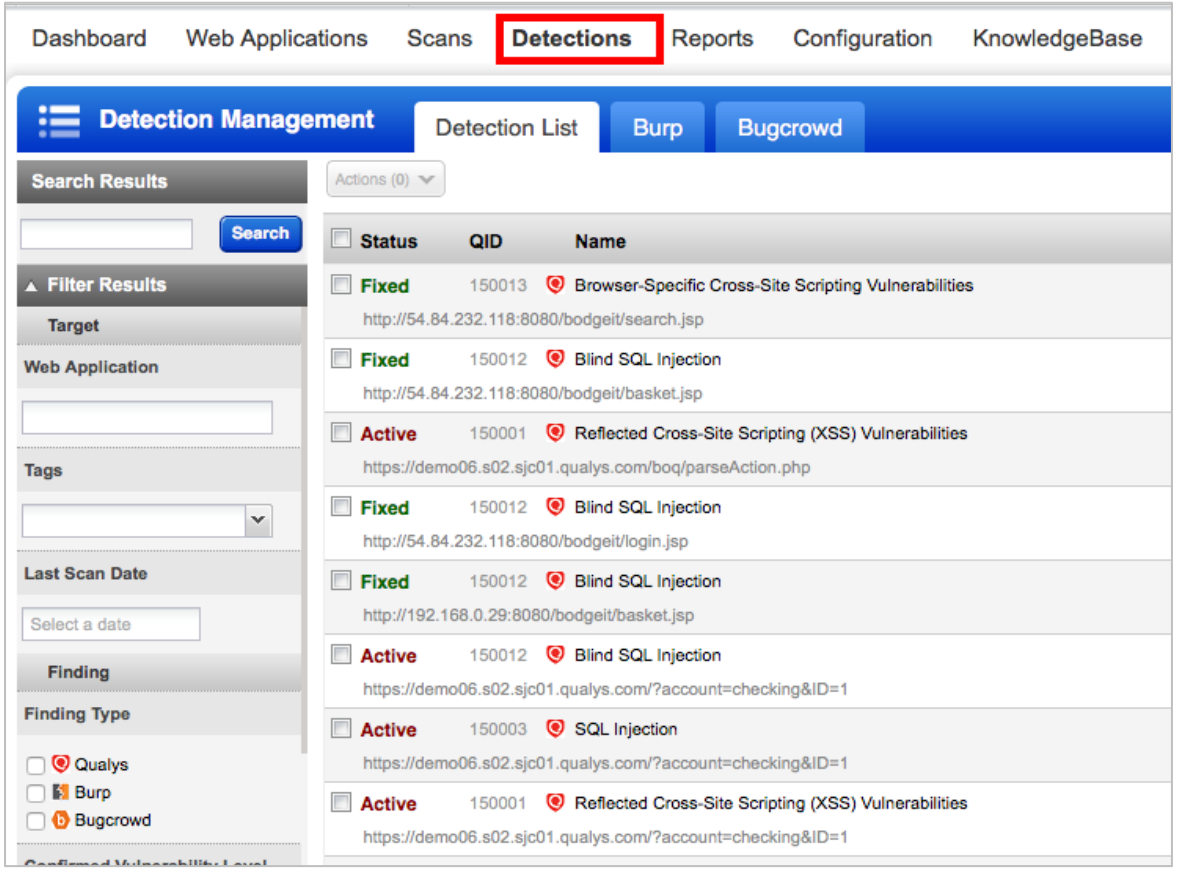
Direct Links:

- Lab 12 – Tagging
- Lab 13 – Users

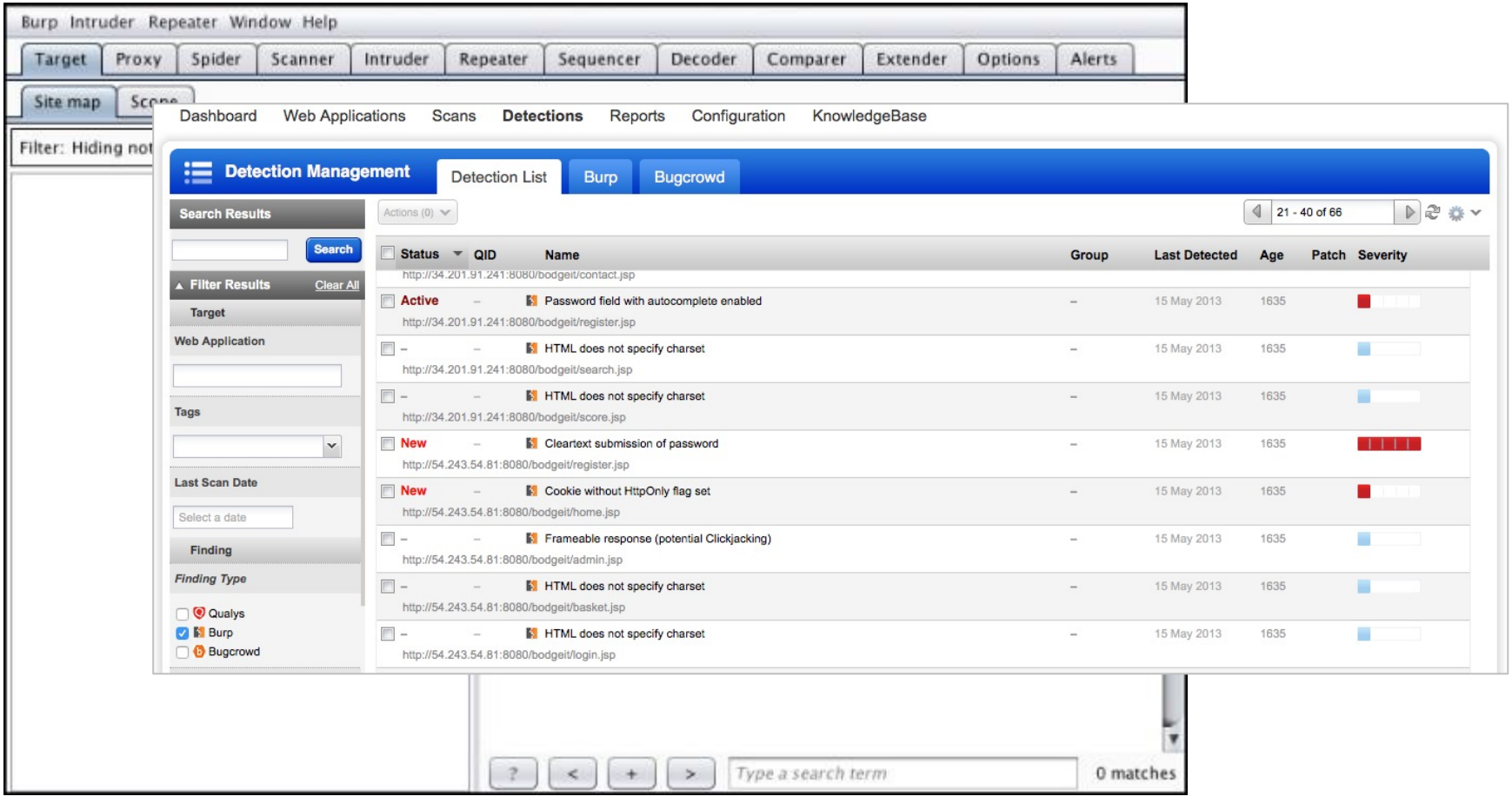
Burp and Bugcrowd Integration

WAS Integration

- Centralized location for vulnerability details.

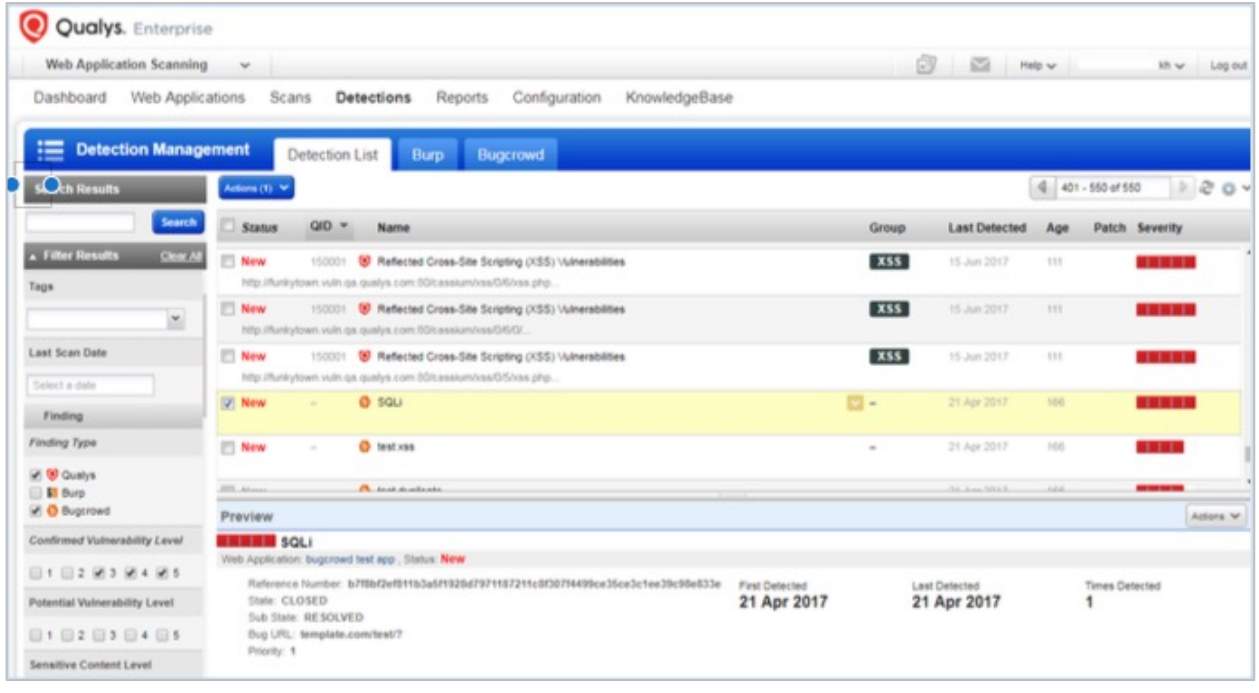


Burp Suite Professional Integration



Bugcrowd Integration

- Qualys WAS and Bugcrowd can now bi-directionally import and export findings



Web Malware Detection

Malware Detection

You plug in your URL

↓

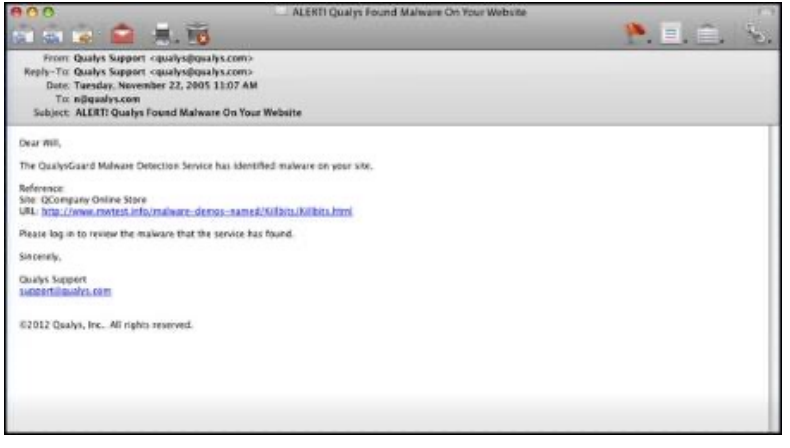
Malware Detection Service

↓

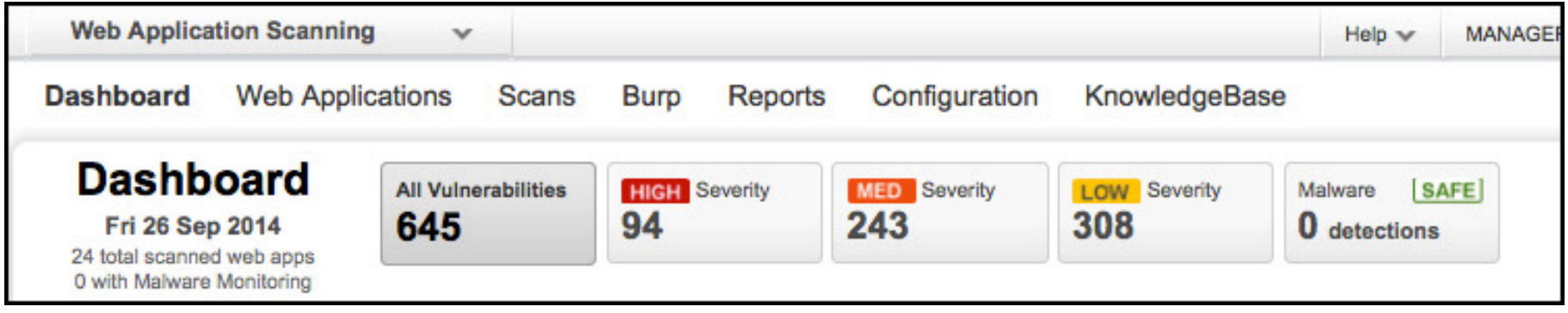
Qualys Virtual Machine Farm

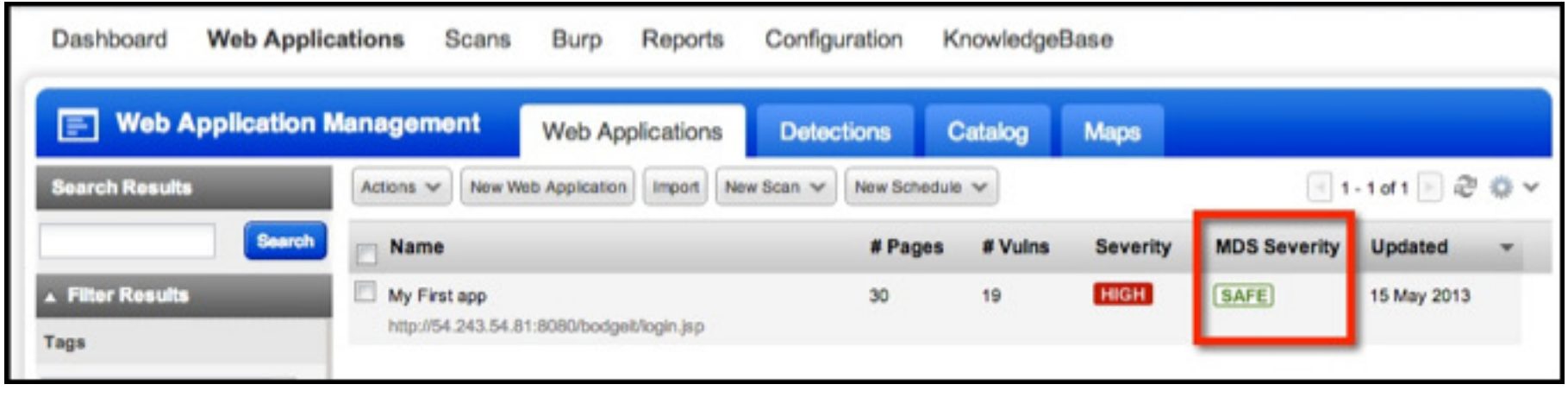
→

1. Enter URL
2. MDS does a breadth crawl URL (we stay in the domain).
3. MDS runs both behavioral and static analysis.
4. Qualys will email user if Malware is found.



Malware Detection





Lab 14

Please follow **page 27** from the Lab Tutorial Supplement

Lab Supplement - https://bit.ly/qsc2021-was

Lab 14 – Burp Integration

Course Survey

Qualys®

Thank You

training@qualys.com